Call Blocking Tools Available to Consumers:
Second Report on Call Blocking
CG Docket No. 17-59

A Report of the Consumer and Governmental Affairs Bureau
Federal Communications Commission
June 2021

TABLE OF CONTENTS

I. INTRODUCTION

1. Illegal and unwanted calls, including robocalls, are the single largest source of consumer complaints to the FCC. In June 2020, the Commission's Consumer and Governmental Affairs Bureau (Bureau), in consultation with the Wireline Competition Bureau and Public Safety and Homeland Security Bureau, released a Staff Report on the state of deployment of advanced methods and tools to eliminate such calls.[1] The report detailed the state of call blocking products and services offered by voice service providers and data analytics companies in the United States. The report also included information on the state of deployment of caller ID authentication through implementation of the STIR/SHAKEN framework and contained other "snapshots" of deployment and implementation of Commission and industry efforts at the time of release.

2. The Commission remains committed to working with industry and other government agencies to eliminate the scourge of illegal robocalls. As required by the *2019 Call Blocking Declaratory Ruling*,[2] and again in consultation with the Wireline Competition Bureau and Public Safety and Homeland Security Bureau, the Bureau has prepared this Second Call Blocking Report to provide an update on deployment and implementation of call blocking and caller ID authentication since the release of the First Call Blocking Report.[3] This Second Call Blocking Report compiles detailed information on a number of call blocking issues such as the availability and effectiveness of call blocking tools offered to consumers,

[1] *Call Blocking Tools Now Substantially Available to Consumers: Report on Call Blocking*, CG Docket No. 17-59, A Report of the Consumer and Governmental Affairs Bureau, Federal Communications Commission, June 2020 (First Call Blocking Report).

[2] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876, 4904, para. 87 (2019) (*2019 Call Blocking Declaratory Ruling*) (requiring that the Bureau within 12 and 24 months prepare two reports "on the state of deployment of advanced methods and tools to eliminate such calls, including the impact of call blocking on 911 and public safety").

[3] The Commission required the Bureau to prepare these two reports in the *2019 Call Blocking Declaratory Ruling*.

the impact of the Commission's actions on illegal calls, and the impact of call blocking on 911 services and public safety. The Second Call Blocking Report presents updated information from a number of sources identified herein, including comments submitted by voice service providers, third-party analytics companies, and others.[4]

3. As we discuss in more detail below, many voice service providers and third-party analytics companies offer improved call blocking services to their customers to protect them from illegal and unwanted calls. Voice service providers and third-party analytics companies use new data continually to update their analyses to detect robocalls; they report offering consumers more blocking tools and blocking more calls. But not all consumers have opted into many of the call blocking technologies offered by providers. Voice service providers and analytics companies report few false positives, i.e., calls incorrectly identified as being spam or fraudulent, and then being blocked in error. They report that they have found no public safety issues related to call blocking. Further, voice service providers report progress in deploying STIR/SHAKEN caller ID authentication on the Internet Protocol (IP) portions of their networks.

4. Despite the progress outlined herein, robocalls remain a substantial consumer problem. The call blocking and caller ID authentication tools discussed in this Second Call Blocking Report are not the only solutions the Commission is pursuing in its effort to stop unwanted and illegal calls. As discussed below, the Commission has taken a multi-pronged approach that includes aggressive enforcement, consumer education, and creating an effective regulatory environment that enables and encourages phone companies and others to proactively stop unwanted robocalls from ever reaching customers. Going forward, the Commission will build on this foundation and continue to use every tool at its disposal to combat and prevent illegal robocalls.

II. BACKGROUND

5. Robocalls are calls made using certain automated equipment.[5] Unwanted robocalls annoy consumers, and can be a vehicle for fraud;[6] so much so that many consumers have stopped answering their telephones when they do not recognize the caller's number.[7] Unwanted robocalls also threaten public safety by disrupting emergency medical communications and 911 call centers, also known

[4] Third-party analytics companies provide various call blocking and labeling services, and caller ID, directly to consumers and through voice service providers. *See, e.g.*, Hiya, *Who we are and what we're about*, https://www.hiya.com/about (last visited June 15, 2021); YouMail, *Block spammers, telemarketers, and unwanted calls forever*, https://www.youmail.com/home/feature/call-blocker (last visited June 15, 2021). The Commission does not regulate third-party analytics companies.

[5] Robocalls are calls made using an automatic telephone dialing system (often referred to as an autodialer) or an artificial or prerecorded voice. The Telephone Consumer Protection Act (TCPA) defines "automatic telephone dialing system" as "equipment which has the capacity(A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers." 47 U.S.C. § 227(a)(1). The Supreme Court has recently clarified that "a necessary feature of an autodialer under § 227(a)(1)(A) is the capacity to use a random or sequential number generator to either store or produce phone numbers to be called." *Facebook, Inc. v. Duguid*, No. 19-511, 2021 WL 1215717 at *7 (Apr. 1, 2021).

[6] *See, e.g.*, Press Release, Department of Justice, U.S. Attorney's Office, Eastern District of Virginia, Two Men Plead Guilty in Multimillion-Dollar International Robocalls Scheme, (Feb. 22, 2021), https://www.justice.gov/usao-edva/pr/two-men-plead-guilty-multimillion-dollar-international-robocalls-scheme.

[7] Third-party analytics company Hiya estimates that 94% of calls from an unknown caller are not answered. *See* https://www.hiya.com/ (last visited June 15, 2021).

[8] *See Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97, 20-67, Report and Order and Further Notice (continued….)

as Public Safety Answering Points (PSAPs).[8] It is no wonder, then, that the Commission has made stopping unlawful robocalls its highest consumer protection priority.[9]

6. Voice service providers and third-party analytics companies offer call blocking tools to prevent unwanted calls from ever reaching consumers.[10] These tools enable consumers to block calls from specific numbers[11] and from numbers providers believe are highly likely to be illegal.[12] As we discuss below, voice service providers and analytics companies also offer call labeling as another tool to assist consumers. Call labeling displays categories for potentially unwanted or illegal calls such as "spam" or "scam likely" on the device's screen, enabling the called party to make a more informed decision about whether to answer.

7. *Complaints.* The Commission receives thousands of informal consumer complaints each year about unwanted calls, including robocalls; it is the Commission's top category of consumer complaints.[13] The Commission received approximately 150,000 such complaints in 2016, 185,000 in 2017, 232,000 in 2018, 193,000 in 2019, and 157,000 in 2020.[14] For 2021, the Commission received

---

of Proposed Rulemaking, 35 FCC Rcd 3241, 3264, para. 50 (2020) (*STIR/SHAKEN Order*) (discussing the impact of robocalls on emergency and healthcare communications).

[9] FCC, *Stop Unwanted Robocalls and Texts*, https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts?from=home#call-blocking-resources (last visited June 15, 2021); FCC, *The FCC's Push to Combat Robocalls & Spoofing*, https://www.fcc.gov/about-fcc/fcc-initiatives/fccs-push-combat-robocalls-spoofing (last visited June 15, 2021).

[10] Call blocking is "stopping calls outright so that they do not ring a phone, routing the calls directly to voicemail without ringing the phone, or some other treatment, such as interactive voice response session or voice call screening." *2019 Call Blocking Declaratory Ruling*, 34 FCC Rcd at 4884 n.47.

[11] *See, e.g.*, Verizon, *Add a Block-Call & Message Blocking-My Verizon Website*, https://www.verizonwireless.com/support/knowledge-base-200867/ (last visited June 15, 2021); Verizon, *Helping our Customers Block Robocalls*, https://www.verizon.com/about/responsibility/robocalls (last visited June 15, 2021); AT&T, *Block Unwanted Wireless Calls and Messages*, https://www.att.com/support/article/wireless/KM1009412/ (last visited June 15, 2021); AT&T, *AT&T Call Protect Expands Service, Automatic Blocking of Fraud Calls Coming to Millions of AT&T Customers*, (July 9, 2019), https://about.att.com/story/2019/att_call_protect.html; Vonage, *Selective Call Block*, https://www.vonageforhome.com/personal/features/selective-call-block/ (last visited June 15, 2021).

[12] *See, e.g.*, some call blocking apps offered by third-party analytics companies and voice service providers for wireless phones: Hiya, *Caller ID, Call Blocker*, https://www.hiya.com/ (last visited June 15, 2021); Nomorobo, *Stop Robocalls and Telemarketers*, https://www.nomorobo.com/ (last visited June 15, 2021); RoboKiller, *Start Blocking Robocalls with RoboKiller Now*. https://app.robokiller.com/ (last visited June 15, 2021); YouMail, *Protect Every Call and Delight Important Callers*, https://www.youmail.com/home/features (last visited June 15, 2021); AT&T, *Get Info on AT&T Call Protect*, (Jan. 14, 2021) https://www.att.com/support/article/wireless/KM1252907; Verizon, *Call Filter, Answer with Confidence*, https://www.verizon.com/solutions-and-services/call-filter/ (last visited June 15, 2021).

[13] FCC, *Consumer Complaint Data Center*, https://www.fcc.gov/consumer-help-center-data (last visited June 15, 2021). We also note that pursuant to the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, 133 Stat. 3274 (Dec. 30, 2019) (TRACED Act), the Commission described consumer complaint data received since 2015 in a report to Congress. *See* "Report To Congress On Robocalls And Transmission Of Misleading Or Inaccurate Caller Identification Information," prepared by the Enforcement Bureau, Consumer and Governmental Affairs Bureau, and Wireline Competition Bureau, submitted pursuant to sections 3, 11, and 13 of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (Dec. 23, 2020), https://docs.fcc.gov/public/attachments/DOC-368957A1.pdf.

[14] FCC, *Consumer Complaint Data Center*, https://www.fcc.gov/consumer-help-center-data (last visited June 15, 2021). The complaint numbers declined significantly during the first four months of the COVID-19 pandemic in 2020, reducing the total number of complaints the Commission received that year. *Advanced Methods to Target and*

(continued….)

approximately 14,000 unwanted call complaints in January, 15,000 in February, 18,000 in March, 16,000 in April, and 15,000 in May.

8. Consumers also complain to the Federal Trade Commission (FTC), which received 480,559 complaints in March 2021.[15] In addition, third-party analytics companies track unwanted robocalls.[16] Hiya reports that 62% of consumers knowingly received a spoofed[17] call in 2020.[18] YouMail estimates that robocallers made 30.5 billion robocalls in 2017, 47.8 billion in 2018, 58.5 billion in 2019, 45.9 billion in 2020, and 22 billion so far in 2021.[19]

9. *Commission rulemaking—call blocking initiatives.* Prior to 2017, the Commission had concluded that call blocking without consumer consent was generally an unjust and unreasonable practice under section 201(b) of the Communications Act of 1934, as amended (Communications Act).[20] Since 2017, however, the Commission has authorized voice service providers to block certain calls without consumers' consent.[21] In the *2017 Call Blocking Report and Order*, the Commission authorized voice service providers to block at the network level (i.e., without consumer consent) calls purporting to be from invalid, unallocated, or unused numbers and numbers on a Do-Not-Originate (DNO) list.[22] This was

(Continued from previous page)
Eliminate Unlawful Robocalls, CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd 15221, 15222 n.3 (2020) (*Calling Blocking Fourth Report and Order*).

[15] *See* National Do Not Call Registry, *All Complaints by Call Type*, https://public.tableau.com/profile/federal.trade.commission#!/vizhome/DoNotCallComplaints/Maps (last visited June 15, 2021).

[16] YouMail extrapolates the data it collects from its user bases to estimate the volume of calls in the United States. For example, according to YouMail, there were four billion robocalls placed in January 2021. YouMail, *January 2021 Nationwide Robocall Data*, https://robocallindex.com/ (last visited June 15, 2021).

[17] Scammers often use spoofing, i.e., altering the caller ID information that appears on the called party's phone display, to maliciously impersonate businesses or governmental agencies. *See* FCC, *Caller ID Spoofing*, https://www.fcc.gov/spoofing (last visited June 15, 2021); FCC, *Combatting Spoofed Robocalls with Caller ID Authentication*, https://www.fcc.gov/call-authentication (last visited June 15, 2021).

[18] Hiya, *State of the Call*, https://hiya.com/state-of-the-call (last visited June 15, 2021).

[19] YouMail, *Historical Robocalls By Time*, https://robocallindex.com/history/time (last visited June 15, 2021).

[20] *See, e.g.*, *Connect America Fund, A National Broadband Plan for Our Future, Establishing Just and Reasonable Rates for Local Exchange Carriers, High-Cost Universal Service Support, Developing an Unified Intercarrier Compensation Regime, Federal-State Joint Board on Universal Service, Lifeline and Link-Up, Universal Service Reform-Mobility Fund*, Report and Order and Further Notice of Proposed Rulemaking, 26 FCC Rcd 17663, 17903, para. 734 (2011) ("The Commission has a longstanding prohibition on call blocking."); *Establishing Just and Reasonable Rates for Local Exchange Carriers, Call Blocking by Carriers*, WC Docket No. 07-135, Declaratory Ruling and Order, 22 FCC Rcd 11629, 11629, para. 1 (WCB 2007) (noting "the Commission's general prohibition on call blocking" and clarifying the obligation of interexchange carriers and commercial mobile radio service providers to complete their customers' interexchange calls). However, the Commission recognized that call blocking has been permitted since at least 1991 to prevent fraud or with consumer approval. *See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, WC Docket No. 07-135, Declaratory Ruling and Order, 30 FCC Rcd 7961, 8036-37, para. 158 (2015); *see also 2019 Call Blocking Declaratory Ruling*, 34 FCC Rcd at 4883-84, para. 22.

[21] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, WC Docket No. 17-97, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706 (2017) (*2017 Call Blocking Report and Order*); *2019 Call Blocking Declaratory Ruling* 34 FCC Rcd at 4886-88, paras. 33-34; 47 CFR § 64.1200(k)(1), (2).

[22] *2017 Call Blocking Report and Order*, 32 FCC Rcd at 9710-21, paras. 10-40. Phone numbers that are only used by their subscribers to receive inbound calls can be placed on a DNO list. These subscribers are generally government and enterprise users with call centers that receive calls on a specific toll-free number that is not used to
(continued….)

an important step in preventing robocalls because, for the first time, it gave voice service providers the option of blocking calls that are "highly likely to be illegal" without the consent of consumers.[23]

10. In the *2019 Call Blocking Declaratory Ruling*, the Commission clarified that voice service providers may offer call blocking services on an opt-out basis (i.e., by default without consumers having to take any action) to new and existing customers, and that such services may block calls where the blocking is based on reasonable analytics designed to identify unwanted calls.[24] Most voice service providers also offer call blocking and labeling services on an opt-in or opt-out basis, generally through a third-party analytics company.[25] Consumers can also obtain call blocking and labeling services directly from third-party analytics companies.[26]

11. Safe harbors for voice service providers encourage call blocking where providers could inadvertently block certain calls.[27] In addition to adopting safe harbor rules,[28] the Commission recently required voice service providers to meet certain affirmative obligations and to better police their networks against illegal calls.[29] Specifically, every voice service provider must: (1) respond to traceback requests from the Commission, civil and criminal law enforcement, and the Consortium;[30] (2) take steps to

(Continued from previous page)
make outbound calls. When the subscriber's number is spoofed without the subscriber's consent, the calls purporting to be from that number are most likely illegal. *Id*. at 9710, para. 10.

[23] *2017 Call Blocking Report and Order*, 32 FCC Rcd at 9710, 9713, 9715, paras. 10, 18, 23.

[24] *2019 Call Blocking Declaratory Ruling*, 34 FCC Rcd at 4886-88, paras. 33-34. Subsequently, the Commission stated that terminating voice service providers may block calls at the network level, without consumer opt-in or opt-out, if that blocking is based on reasonable analytics that incorporate caller ID authentication information designed to identify calls and call patterns that are highly likely to be illegal. *Calling Blocking Fourth Report and Order*, 35 FCC Rcd at 15236, para. 42. USTelecom—The Broadband Association filed a Petition for Reconsideration on May 6, 2021. *See Petition of Reconsideration of Action in Proceedings*, CG Docket No. 17-59, Public Notice, (CGB May 11, 2021), https://www.fcc.gov/document/petition-reconsideration-action-proceeding-16.

[25] *See* section III, below, for a discussion of the various blocking and labeling services offered to consumers.

[26] *2019 Call Blocking Declaratory Ruling*, 34 FCC Rcd at 4884-90, paras. 26-42. To opt out is to affirmatively choose not to participate. In this context, the consumer is automatically enrolled in the call blocking service, but can elect to not subscribe to that service. The Commission clarified that voice service providers may offer white list programs on an opt-in basis, i.e., blocking calls from numbers not in a consumer's contacts list. *Id.* at 4890-91, paras. 43-46.

[27] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614, 7623-37, paras. 20-60 (2020) (*Call Blocking Third Report and Order*) (granting voice service providers more incentive to block illegal calls by protecting them from liability resulting from the inadvertent blocking of wanted calls in certain cases). The Commission also expanded the call blocking safe harbor to cover network-based blocking of certain calls that are highly likely to be illegal. *Calling Blocking Fourth Report and Order*, 35 FCC Rcd at 15234-38, paras. 39-47.

[28] The *Call Blocking Fourth Report and Order* expanded the reasonable analytics safe harbor to include network-level blocking, without consumer opt in or opt out, based on reasonable analytics that incorporate caller ID authentication information designed to identify calls and call patterns that are highly likely to be illegal, so long as certain safeguards are in place, such as providing human oversight and network monitoring. *See* 47 CFR § 64.1200(k)(11); *Call Blocking Fourth Report and Order*, 35 FCC Rcd at 15234-36, paras. 39-43.

[29] *Calling Blocking Fourth Report and Order*, 35 FCC Rcd at 15227-234, paras. 14-38; *Call Blocking Third Report and Order*, 35 FCC Rcd at 7623-37, paras. 20-60.

[30] *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-22, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3113 (2020) (*Traceback Consortium Order*) (adopting rules for a registration process for a consortium to conduct private-led traceback initiatives); *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse*
(continued….)

effectively mitigate illegal traffic when it receives actual written notice of such traffic from the Commission; and (3) implement affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls.[31]

12. The Commission adopted rules to provide greater transparency and ensure that both callers and consumers can better identify blocked calls and obtain effective redress when wanted calls are blocked, as required by section 10(b) of the TRACED Act.[32] Finally, the Commission broadened the point-of-contact requirement to cover complaints from callers adversely affected by information provided by caller ID authentication, as required by section 4(c)(1)(C) of the TRACED Act.[33]

13. As required by the TRACED Act, the Commission enabled blocking of calls associated with a specific type of call—the one-ring scam.[34] A one-ring scam is a call, "in which a caller makes a call and allows the call to ring the called party for a short duration, in order to prompt the called party to return the call, thereby subjecting the called party to charges."[35] The Commission expressly enabled voice service providers to block calls from numbers highly likely to be associated with a one-ring scam.[36]

14. *Commission rulemaking—STIR/SHAKEN actions*. The TRACED Act also directed the Commission to require voice service providers to "implement the STIR/SHAKEN authentication framework" in the portions of their networks using IP, and to "take reasonable measures to implement an effective call authentication framework" in the non-IP portions of their networks no later than June 30, 2021.[37] STIR/SHAKEN[38] is a framework developed for IP networks to authenticate caller ID information and should reduce the effectiveness of illegal spoofing.[39] Illegal caller ID spoofing, i.e., falsifying the caller ID information that appears on the called party's phone with the intent to defraud, cause harm, or wrongfully obtain anything of value, can often be the key to a robocall scam's success.[40] One tool to combat illegal caller ID spoofing is caller ID authentication, which allows voice service providers to

(Continued from previous page)
Criminal Enforcement and Deterrence Act (TRACED Act), EB Docket No. 20-22, Report and Order, 35 FCC Rcd 7886 (EB 2020) (*ITG Consortium Order*) (selecting USTelecom's Industry Traceback Group as the consortium to conduct private-led traceback efforts). The consortium is a group of voice service providers, wireline, wireless, and VoIP, that are tracing and identifying the source of illegal robocalls. For the latest Industry Traceback Report, *see* Industry Traceback Group, *Combatting Illegal Robocalls*, https://www.ustelecom.org/research/combatting-illegal-robocalls/ (last visited June 15, 2021).

[31] *Calling Blocking Fourth Report and Order*, 35 FCC Rcd at 15227, para. 14; 47 CFR § 64.1200(n).

[32] *Calling Blocking Fourth Report and Order*, 35 FCC Rcd at 15238-249, paras. 48-73.

[33] *Id.*, 35 FCC Rcd at 15246-47, paras. 74-78.

[34] *See Protecting Consumers from One-Ring Scams*, CG Docket No. 20-93, Report and Order, 35 FCC Rcd 14236 (2020) (*One-Ring Scam Report and Order*).

[35] TRACED Act, § 12(d)(1).

[36] 47 CFR § 64.1200(k)(2)(iv).

[37] TRACED Act, § 4(b)(1)(A), (B). In addition, the TRACED Act provides that "[t]he Commission shall prohibit providers of voice service from adding any additional line-item charges to consumer or small business customer subscribers for the effective call authentication technology required." TRACED Act, § 4(b)(6). *See STIR/SHAKEN Order*; 35 FCC Rcd at 3252-3260, paras. 24-41.

[38] SHAKEN, or Signature-based Handling of Asserted information using toKENS, and STIR, or Secure Telephony Identity Revisited, uses public key cryptography to provide assurances that certain information about the transmitted caller ID is accurate. *2019 Call Blocking Declaratory Ruling*, 34 FCC Rcd at 4883, para. 21.

[39] *Id.*, 34 FCC Rcd at 4883, para. 21.

[40] *2017 Call Blocking Report and Order*, 32 FCC Rcd at 9707, para. 3.

verify that the caller ID information transmitted with a particular call matches the caller's number, which in turn helps to determine whether the call should be blocked or labeled.[41]

15. Subsequently, the Commission established extension and exemption mechanisms for various categories of providers and made clear the obligations on voice service providers to protect the non-IP parts of their networks, including by developing non-IP caller ID authentication solutions.[42] Once a provider has implemented STIR/SHAKEN standards, it can attest to all IP-based calls that originate on or transit its network by adding a Session Initiation Protocol (SIP) header containing specific information, which is then transmitted in encrypted form with the call to the terminating provider.[43] The terminating voice service provider uses this additional information to verify that the caller ID information transmitted with a call matches the caller's number.[44]

16. The Commission established the Robocall Mitigation Database, which opened in April 2021, and requires "all voice service providers to file certifications with the Commission regarding their efforts to stem the origination of illegal robocalls on their networks."[45] The Wireline Competition Bureau set June 30, 2021 as the deadline for voice service providers to submit required information to the Robocall Mitigation Database.[46] The Commission's rules prohibit intermediate providers and terminating voice service providers from accepting traffic from voice service providers not listed in the Robocall Mitigation Database beginning September 28, 2021.[47]

17. *Commission rulemaking—TCPA, section 8 of the TRACED Act, and the Reassigned Numbers Database*. In the 2019 TRACED Act, Congress enacted further measures to combat robocalls.[48] Pursuant to the requirements in the TRACED Act, the Commission established a Traceback Consortium, created the Hospital Robocall Protection Group,[49] and implemented stronger enforcement provisions for

[41] STIR/SHAKEN allows providers to transmit calls with three levels of attestation: a voice service provider can indicate that (i) it can confirm the identity of the subscriber making the call, and that the subscriber is using its associated telephone number ("A" or "full" attestation); (ii) it can confirm the identity of the subscriber but not the telephone number ("B" or "partial" attestation); or merely that (iii) it is the point of entry to the IP network for a call that originated elsewhere, such as a call that originated abroad or on a domestic network that is not STIR/SHAKEN-enabled ("C" or "gateway" attestation). *STIR/SHAKEN Order*, 35 FCC Rcd at 3245, para. 8.

[42] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1892-96, paras. 66-70 (2020) (*Second STIR/SHAKEN Order*). More recently, the Commission has considered shortening the existing two-year extension for small providers that are most likely to be responsible for originating illegal robocalls. *Call Authentication Trust Anchor*, WC Docket No. 17-97, Third Further Notice of Proposed Rulemaking, FCC 21-62, at paras. 13-19 (2021) (*STIR/SHAKEN Third FNPRM).*

[43] *Second STIR/SHAKEN Order*, 36 FCC Rcd at 1863-64, paras. 8-10.

[44] *Id.*, 36 FCC Rcd at 1863, para.8.

[45] *Id.*, 36 FCC Rcd at 1902, para. 82.

[46] 47 CFR § 64.6305(b).

[47] *Wireline Competition Bureau Announces Opening Of Robocall Mitigation Database And Provides Filing Instructions And Deadlines*, WC Docket No 17-97, Public Notice, DA 21-454 (WCB Apr. 20, 2021).

[48] The TRACED Act was adopted on Dec. 30, 2019. The Commission has a web page detailing the steps it has taken to implement the TRACED Act. *See* FCC, *TRACED Act Implementation*, https://www.fcc.gov/TRACEDAct (last visited June 15, 2021).

[49] The Hospital Robocall Protection Group is required by section 14 of the TRACED Act. *See FCC Concludes Best Practices to Combat Unlawful Robocalls to Hospitals*, Public Notice, DA 21-688 (CGB June 11, 2021); News Release, FCC, Hospital Robocall Protection Group Adopts Best Practices Report On Preventing Unlawful Calls, Recommendations Focus on Voice Service Providers, Hospitals, and Federal and State Governments Collaborating on Prevention, Response, and Mitigation, (Dec. 14, 2020), https://www.fcc.gov/document/hospital-robocall-protection-group-issues-best-practices.

illegally spoofed calls and for robocalls made with the intent to violate section 227(b) of the Act.[50] In addition, the TRACED Act directed the Attorney General, in consultation with the Chair of the FCC, to convene an interagency working group to study prosecutions under section 227(b) of the Communications Act.[51]

18. The Commission also recently adopted a Report and Order creating an online portal to allow entities to submit information about robocalls and caller ID spoofing, as directed by section 10 of the TRACED Act.[52]

19. In addition, the Commission has addressed the related issue of consumers with a telephone number that was reassigned from a prior customer who gave consent to be called. In December 2018, the Commission authorized the creation of the Reassigned Numbers Database to enable callers to verify whether a telephone number has been permanently disconnected, and is therefore eligible for reassignment, before calling that number, thereby helping to protect consumers with a reassigned number from receiving unwanted calls.[53] The Commission selected SomosGov, Inc. to develop and administer the Reassigned Numbers Database and work began in December 2020. Service providers began reporting

[50] *Amendment of Section 1.80 of the Commission's Rules*, Order, 35 FCC Rcd 4476 (EB 2020) (adopting stronger enforcement provisions for illegal robocalls). In the *Section 8 TRACED Act Order*, the Commission also amended the rules for TCPA exemptions for calls made to residential telephone lines to ensure each satisfies section 8(a) of the TRACED Act's requirement to identify who can call, who can be called, and any call limits. *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 35, FCC Rcd 15188 (2020) (*Section 8 TRACED Act Order*). The exemptions are for: (1) non-commercial calls to a residence; (2) commercial calls to a residence that do not include an advertisement or constitute telemarketing; (3) tax-exempt nonprofit organization calls to a residence; and (4) HIPAA-related calls to a residence. *Section 8 TRACED Act Order*, 35 FCC Rcd at 15192-15200, paras. 12-40.

[51] TRACED Act § 5; Press Release, U.S. Department of Justice, Telephone Robocall Abuse Criminal Enforcement and Deterrence Act 2020 Report to Congress, https://www.justice.gov/opa/press-release/file/1331576/download (last visited June 15, 2021).

[52] *Implementing Section 10(a) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-374, Report and Order, FCC 21-75 (rel. June 17, 2021). In addition, the Bureau has adopted declaratory rulings confirming that the TCPA applies to any telephone call to a residential telephone line initiated using an artificial or prerecorded voice message. *See, e.g.*, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Declaratory Ruling and Order, 35 FCC Rcd 14640 (CGB 2020) (affirming that if the call is initiated using an artificial or prerecorded voice message—whether made using soundboard technology or otherwise—the caller must obtain the called party's prior express consent for such a call unless an exemption applies).

[53] The Database will provide comprehensive and timely information to enable callers to avoid making calls to reassigned numbers. *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, WC Docket No. 17-97, Second Report and Order, 33 FCC Rcd 12024, 12029-35, paras. 11-27 (2018) (*Robocall Second Report and Order*); *Consumer And Governmental Affairs Bureau Announces Compliance Date For Remaining Reassigned Numbers Database Rule Regarding Reporting Of Disconnect Data*, CG Docket No. 17-59, Public Notice, 36 FCC Rcd 1441 (CGB 2021); *Consumer And Governmental Affairs Bureau Announces Technical Specifications For Reassigned Numbers Database Reporting*, CG Docket No. 17-59, Public Notice, 36 FCC Rcd 316 (CGB 2021); *Report To Congress Reassigned Number Database, Status of Commission Efforts Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Consumer and Governmental Affairs Bureau, Submitted to the United States Congress pursuant to section 9 of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (Dec. 8, 2020), https://docs.fcc.gov/public/attachments/DOC-368620A1.pdf.

information about disconnected telephone numbers on April 15, 2021.[54] After a soft launch this summer, we expect that callers will be able to use the Reassigned Numbers Database this fall.[55]

20. *Enforcement.* In addition to TRACED Act implementation and other rulemakings, the Commission has taken aggressive enforcement action against illegal robocallers.[56] In 2020, the Commission learned that robocall scammers were capitalizing on public anxiety about the COVID-19 pandemic by making robocalls to sell nonexistent COVID-19 testing kits, among other things.[57] On April 3, 2020 and May 20, 2020, the Commission and the FTC jointly sent warning letters to five gateway providers and one originating provider demanding that they cease carrying fraudulent COVID-19-related robocall traffic.[58] The Commission has also taken enforcement action concerning robocalls more generally. On March 17, 2021, the Enforcement Bureau issued six cease-and-desist letters to companies that appeared to transmitting illegal robocalls,[59] and on April 13, 2021, the Enforcement Bureau issued cease-and-desist letters to two companies apparently transmitting unlawful robocall campaigns marketing auto warranties and credit card debt reduction service, or falsely claiming to be from the Social Security Administration or well-known companies.[60] Recently, on May 18, 2021, the Enforcement Bureau issued two cease-and-desist letters to companies and ordered that that they immediately cease carrying illegal

[54] Small providers have until October 15, 2021 to submit their data. *Consumer and Governmental Affairs Bureau Announces Compliance Date for Remaining Reassigned Numbers Database Rule Regarding Reporting of Disconnect Data*, CG Docket No. 17-59, Public Notice, 36 FCC Rcd 1441 (CGB 2021).

[55] *Consumer and Governmental Affairs Bureau Announces Beta Test for Users of the Reassigned Numbers Database Rule Regarding Reporting of Disconnect Data*, CG Docket No. 17-59, Public Notice, DA 21-699 (CGB June 15, 2021).

[56] *See, e.g.*, *John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC, et. al.,* Forfeiture Order, FCC 21-35 (Mar. 14, 2021) (adopting the largest forfeiture in FCC history, $225,000,000, against persons apparently responsible for making approximately one billion spoofed robocalls in the first four-and-a-half months of 2019 that included prerecorded messages falsely claiming affiliation with major health insurance providers in the United States); *Scott Rhodes a.k.a. Scott David Rhodes, Scott D. Rhodes, Scott Platek, Scott P. Platek*, Forfeiture Order, 36 FCC Rcd 705 (2021) (adopting a forfeiture of $9,918,000 for spoofed robocalls in six campaigns with hate speech and racist, anti-Semitic, or anti-immigrant language, using spoofed numbers belonging to innocent parties that matched the locality of the called party); *Kenneth Moser dba Marketing Support Systems*, Forfeiture Order, 35 FCC Rcd 13415 (2020) (adopting a forfeiture of $9,997,750 for calls made spoofing the telephone number of another telemarketing company with a prerecorded message containing false statements critical of a state assembly candidate).

[57] *See* Tony Romm, *'That can actually kill somebody': Scam robocalls are pitching fake coronavirus tests to vulnerable Americans*, Washington Post (Mar. 19, 2020), https://www.washingtonpost.com/technology/2020/03/19/robocalls-coronavirus-test/.

[58] *See* News Release, FCC, FCC, FTC Demand Gateway Providers Cut Off Robocallers Perpetrating Coronavirus-Related Scams from United States Telephone Network (Apr. 3, 2020), https://www.fcc.gov/document/fcc-ftc-demand-gateway-providers-cut-covid-19-robocall-scammers; News Release, FCC, FCC, FTC Demand Robocall-Enabling Service Providers Cut Off Scammers, (May 20, 2020), https://www.fcc.gov/document/fcc-ftc-demand-robocall-enabling-service-providers-cut-scammers.

[59] News Release, FCC, Acting Chairwoman Rosenworcel Kicks Off Anti-Robocall Agenda; Issues Largest Robocall Fine in FCC History, Demands Providers Cease-and-Desist From Illegal Robocalls, Launches Robocall Response Team, Renews Federal-State Collaboration (Mar. 17, 2021), https://www.fcc.gov/document/acting-chairwoman-rosenworcel-kicks-anti-robocall-agenda.

[60] News Release, FCC, FCC Calls On Carriers To Ensure Free Consumer Tools Are Available To Block Robocalls And Issues New Robocall Cease-And-Desist Letters (Apr. 13, 2021), https://docs.fcc.gov/public/attachments/DOC-371553A1.pdf.

robocall campaigns on their networks and report to the Commission the concrete steps they implemented to prevent a recurrence of these operations.[61]

21. *Consumer Education.* The Commission educates consumers on how to avoid illegal robocalls. This includes videos, audio samples from actual scam calls, and tip sheets through our website and social media.[62] The Consumer Help Center's robocall page,[63] which contains tips on how consumers can avoid robocalls, is the Help Center's most visited page, averaging over one million visits annually. The Consumer Help Center also contains a variety of content alerting consumers to new and ongoing scams that rely on spoofed robocalls to defraud consumers.[64] In response to the COVID-19 pandemic, the Commission established a new consumer resource page to highlight pandemic-specific phone-based scams.[65]

22. The Commission has also closely collaborated with the FTC on education and outreach efforts focused on spoofing and illegal robocalls.[66] In addition, the Bureau's Office of Intergovernmental Affairs coordinates activities with state commissions and the National Association of Regulatory Utility Commissioners.

23. The Commission's outreach efforts on unwanted calls include rural tours,[67] partnerships with AARP and the National Asian American Coalition, and a focus on vulnerable communities such as older Americans and those who are linguistically isolated. Consumer education materials are available in English, Spanish, Korean, Traditional Chinese, Tagalog, and Vietnamese.[68] With travel limited due to the COVID-19 pandemic, the FCC hosted a series of webinars focused on protecting consumers from unwanted call and text-based scams, including one on COVID-19 scams that featured the Consumer Financial Protection Bureau and the U.S. Department of Health and Human Services.[69]

---

[61] News Release, FCC, FCC Demands Two Companies Cease-and-Desist Illegal Robocall Campaigns (May 18, 2021), https://www.fcc.gov/document/fcc-demands-two-companies-cease-and-desist-illegal-robocall-campaigns.

[62] *See, e.g.*, FCC, *Coronavirus Scams—Consumer Resources*, https://www.fcc.gov/covid-scams (last visited June 15, 2021); FCC, *COVID-19 Robocall Scams,* https://www.fcc.gov/covid-19-robocall-scams (last visited June 15, 2021); FCC, *Consumer Help Center*, https://www.fcc.gov/consumers (last visited June 15, 2021); FCC, *Consumer Guides*, *Call Blocking Tools and Resources*, https://www.fcc.gov/call-blocking (last visited June 15, 2021).

[63] FCC, *Consumer Guides*, *Stop Unwanted Robocalls and Texts*, https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts (last visited June 15, 2021).

[64] FCC, *Consumer Guides*, *Stop Unwanted Robocalls and Texts*, https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts (last visited June 15, 2021); FCC, *Scam Glossary*, https://www.fcc.gov/scam-glossary (last visited June 15, 2021).

[65] FCC, *Coronavirus Scams—Consumer Resources*, https://www.fcc.gov/covid-scams (last visited June 15, 2021).

[66] *See* FCC, *Consumer Guides*, *Stop Unwanted Robocalls and Texts*, https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts (last visited June 15, 2021). The FTC also has information on its website about robocalls. *See* FTC, *Consumer Information, Robocalls*, https://www.consumer.ftc.gov/articles/0259-robocalls (last visited June 15, 2021). *See also* GAO, *Fake Caller ID Schemes: Information on Federal Agencies' Efforts to Enforce Laws, Educate the Public, and Support Technical Initiatives*, GAO 20-153 (Dec. 2019), https://www.gao.gov/assets/710/703362.pdf (discussing FCC, FTC, and DOJ efforts to combat caller ID spoofing).

[67] FCC, *Rural Tour Highlights—Arizona and New Mexico*, https://www.fcc.gov/rural-tour-dispatches (last visited June 15, 2021).

[68] FCC, *Consumer Guides*, https://www.fcc.gov/consumer-guides (last visited June 15, 2021).

[69] FCC, *A Webinar for Consumers: COVID-19 Scams and Older Adults*, https://www.fcc.gov/news-events/events/2021/02/webinar-consumers-covid-19-scams-and-older-adults (last visited June 15, 2021).

24. Commission staff members also attend a monthly State and National Action Plan (SNAP) telephone conference with staff from state commissions and the National Association of Regulatory Utility Commissioners. The Bureau's Office of Intergovernmental Affairs coordinates on agenda topics with the SNAP conference call Chair and works with FCC bureaus and offices to coordinate speakers to make presentations on key FCC policies, consumer education, and enforcement actions. The Enforcement Bureau coordinates every month with the FTC on robocall enforcement, and the Bureau's Office of Intergovernmental Affairs works to coordinate FCC speakers for presentations on key FCC policies, consumer education, and enforcement actions. All of these actions assist American consumers in avoiding unwanted calls.

25. *This Proceeding.* On April 13, 2021, the Bureau released a public notice seeking comment for this Second Call Blocking Report.[70] The Bureau requested updated information on call blocking issues, including the availability and effectiveness of call blocking tools offered to consumers, the impact of the Commission's actions on illegal calls, and the impact of call blocking on 911 services and public safety. We received 28 comments and responses to our letters seeking information from voice service providers, trade associations, third-party analytics companies, and other interested parties.[71] This Second Call Blocking Report describes call blocking initiatives and progress toward protecting consumers from illegal and unwanted robocalls, particularly any new services offered since the release of the First Call Blocking Report. This Second Call Blocking Report also includes updated information on the state of deployment of caller ID authentication through implementation of the STIR/SHAKEN framework.

III. CALL BLOCKING SERVICES

26. As we discussed in the First Call Blocking Report, most voice service providers block, at the network level, calls from telephone numbers on a DNO list and calls that appear to be from invalid, unallocated, or unused numbers, and many voice service providers also offer additional blocking and labeling services, based on various analytics. Below, we summarize the current availability of blocking and labeling services offered by voice service providers and third-party analytics companies.[72]

A. Voice Service Providers' Services

27. The voice service providers AT&T, Bandwidth, Charter, Comcast, Cox, Frontier, Lumen, TDS Telecom, T-Mobile, US Cellular, Verizon, and Vonage state that they offer free blocking services, often through a third-party analytics company; for example, Nomorobo works with various voice service providers and offers call blocking for VoIP landlines at no charge.[73]

28. *AT&T.* AT&T has a network-based, provider-initiated, call blocking program run by the AT&T Global Fraud Management Organization that blocks suspected illegal calls on AT&T's network and terminating to AT&T and non-AT&T customers by relying on network intelligence and a team of fraud investigators.[74] AT&T has a suspected robocall report, a vital tool for the accurate detection of suspected illegal robocalls on its network, which is updated continuously and allows AT&T to compile information on telephone numbers used to place calls with suspicious characteristics and to then identify

[70] *Consumer And Governmental Affairs Bureau Seeks Input For Second Staff Report On Call Blocking*, CG Docket No. 17-59, WC Docket No. 17-97, Public Notice, DA 21-420 (CGB 2021).

[71] *See* Appendix for a list of commenters.

[72] The descriptions of companies' progress below are based on what they have told us. We have not conducted an independent review of those assertions and thus make no statement about their accuracy.

[73] Nomorobo, https://www.nomorobo.com/ (last visited June 15, 2021). Nomorobo offers blocking services directly to consumers and also offers blocking for wireless phones, at a charge of $1.99 per device, per month.

[74] Letter from Joan Marsh, Executive Vice President Regulatory and State External Affairs, AT&T Services, Inc., to Mika Savir, Consumer and Governmental Affairs Bureau, FCC at 4 (Apr. 30, 2021) (AT&T Letter).

patterns indicative of illegal robocalls.[75] Before blocking a telephone number, AT&T conducts an investigation that includes dialing the suspect telephone number.[76] AT&T has blocked 7.3 billion illegal calls since the program launched in 2016, and approximately 1.4 billion in 2020 alone.[77]

29. AT&T describes Call Protect as a free, opt-out,[78] call blocking and labeling service for AT&T wireless customers that automatically blocks suspected fraud calls in its network.[79] AT&T Call Protect also labels calls from telephone numbers believed to be associated with suspect or potentially unwanted sources, including telemarketers and suspected spam.[80] This is available for consumer and business postpaid wireless customers,[81] AT&T FirstNet, AT&T Prepaid, and Cricket customers, and AT&T Wireless Home Phone customers.[82] Since 2016, AT&T has blocked or labeled nearly three billion suspected fraud calls and more than nine billion other suspect calls through AT&T Call Protect.[83]

30. AT&T states that Call Protect users also have the option to opt into additional free features. For example, users can automatically block those calls identified as "Spam Risk" and send directly to voicemail all calls from telephone numbers not in the user's address book; however, by the end of 2020, fewer than 150,000 AT&T wireless customers had opted in to this direct-to-voicemail feature.[84] AT&T, together with third-party analytics company Hiya, continually monitors the effectiveness of the AT&T Call Protect service and refines the analytics.[85] Users of AT&T Call Protect can view blocked calls in the free AT&T Call Protect app and report information on any of these calls.[86] In addition, AT&T solicits feedback on AT&T Call Protect through a web portal.[87]

31. AT&T Home Phone (VoIP) customers can opt in to AT&T Digital Phone Call Protect at no additional charge; this service automatically blocks suspected fraud calls and sends customers a caller ID alert if a call is suspected to originate from one of several categories of potentially unwanted sources.[88] Customers can view the calls that have been blocked online.[89] From December 2017 through March 2021, AT&T has blocked more than 52 million incoming calls and provided more than 55 million spam warnings to Digital Phone Call Protect users.[90] In 2020, AT&T blocked more than 4.5 million incoming

[75] AT&T Letter at 4.

[76] *Id*.

[77] *Id*.

[78] Fewer than 1% of subscribers have opted out of this service. AT&T Letter at 2.

[79] *Id.* at 1.

[80] *Id*.

[81] AT&T, *Mobile Security*, https://www.att.com/security/security-apps/ (last visited June 15, 2021); AT&T, *Block Unwanted Calls with Call Block (*60)*, https://www.att.com/support/article/local-long-distance/KM1010645/ (last visited June 15, 2021).

[82] AT&T Letter at 2.

[83] *Id*.

[84] *Id*.

[85] *Id*.

[86] *Id*.

[87] *Id*. at 2-3. *See* Hiya, *Submit a Request*, https://hiyahelp.zendesk.com/hc/en-us/requests/new?ticket_form_id=824667 (last visited June 15, 2021).

[88] AT&T Letter at 3.

[89] *Id*.

[90] *Id*.

calls and provided more than 13.8 million spam warnings to Digital Phone Call Protect users.[91] As of March 2021, more than 180,000 customers have opted in to Digital Phone Call Protect.[92]

32. AT&T explains that it also offers the AT&T Smart Call Blocker phone, an AT&T-branded phone with call blocking capabilities that works with any landline voice service and on all wireline networks, including legacy time division multiplexing (TDM) based telephone service, for consumers with caller ID.[93] The AT&T Smart Call Blocker phones block calls at the device level; users can create lists of phone numbers that are either always allowed or always blocked, or can screen automated calls or calls without caller ID before the call is allowed to ring.[94] Since 2017, consumers have purchased approximately 1.9 million AT&T Smart Call Blocker phones.[95]

33. *Bandwidth.* Bandwidth states that it operates a network that is entirely optimized for IP technology; it is predominately an underlying service provider to other IP-based communications service providers.[96] Bandwidth has added STIR/SHAKEN feature functionality, such as enabling intermediate transit identity header and in-bound identity header delivery.[97] Bandwidth supports the use of direct-to-consumer oriented tools, opt-in or opt-out, together with its service provider customers to help avoid the delivery and receipt of illegal robocalls.[98] Bandwidth also reports that it continues to build out its fraud identification capabilities and has tools in its network to block voice traffic that originates from invalid numbers as well as filter against the delivery of readily identifiable SPAM messaging traffic.[99]

34. Bandwidth states that it has an on-boarding screening process designed to prevent potential robocalling companies from becoming Bandwidth customers.[100] Bandwidth currently manages call blocking tools that prevent calls with specific unlawful telephone number characteristics from traversing the Bandwidth network and has development projects to expand its capabilities more holistically.[101] Bandwidth personnel regularly analyze network traffic for unlawful robocall campaigns and use call blocking capabilities when appropriate.[102]

35. *Charter Communications (Charter)*. Charter explains that it automatically blocks, at the network level, calls that appear to originate from numbers on the DNO list.[103] Charter offers Call Guard, an advanced caller ID and robocall-blocking solution, at no charge to Spectrum Voice and Spectrum Business Voice customers, on an opt-out basis.[104] Call Guard uses industry-leading data, STIR/SHAKEN

[91] *Id*.

[92] *Id*.

[93] *Id*.

[94] *Id*.

[95] *Id*.

[96] Letter from David Morken, CEO, Bandwidth Inc., to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 1 (Apr. 30, 2021) (Bandwidth Letter).

[97] Bandwidth Letter at 1.

[98] *Id.* at 2.

[99] *Id*.

[100] *Id*.

[101] *Id*.

[102] *Id*.

[103] Letter from Thomas M. Rutledge, Chairman and CEO, Charter Communications, to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 2 (Apr. 30, 2021) (Charter Letter).

[104] Charter Letter at 1.

call-authentication information, and predictive call-pattern analytics to assess every incoming call and apply a score to each based on its measured level of risk.[105] Charter completed its implementation of the STIR/SHAKEN authentication framework across its entire IP network and continues to work with its industry peers to extend the benefits of STIR/SHAKEN to more consumers.[106]

36. Call Guard automatically blocks calls that score as "highly likely" to be malicious or fraudulent and calls originating from invalid or unallocated numbers.[107] Call Guard sends a "Spam Risk" caller ID alert to the customer when a call scores as "suspicious" or "potentially harmful spam" but there is insufficient information to block.[108] Call Guard's reputational scoring system enables it to block the most egregious robocalls, while ensuring that customers receive the legitimate messages from schools and healthcare providers.[109] Customers can also add specific phone numbers to a list to ensure that those numbers are not blocked by Call Guard.[110] Call Guard's use of STIR/SHAKEN authentication information, machine learning algorithms, and other call-pattern data helps it to update its ratings as call trends and scams evolve over time, enabling it to stay current, effective, and reliable.[111]

37. In April 2020, Charter's Spectrum Mobile service started using Hiya, a call-blocking technology producer, to help mobile phone customers block and identify spam calls.[112] Spectrum Mobile customers can download the opt-in Hiya app, at no charge, and have access to spam ID, manual blocking of specific numbers, and caller ID for businesses.[113] Customers can also upgrade to Hiya's premium app for a fee, to automatically block fraud, spam, and nuisance robocalls, and identify unknown calls based on Hiya's caller directory.[114] Charter also offers Spectrum Voice customers additional opt-in robocall-mitigation tools at no cost which, when enabled, allow them to accept only select calls, block specific unwanted callers, and block anonymous calls.[115]

38. Charter states that it has seen a significant reduction in the number of fraudulent or otherwise harmful calls that reach consumers, a minimal amount of reports of wrongfully blocked calls, and a very small percentage of customers that opt out of the default features.[116] Charter's targeted robocall-blocking tools have blocked tens of millions of calls per month that analytics indicated as the highest risk of being fraudulent, malicious, misleading, or otherwise harmful.[117]

39. *Comcast.* Comcast explains that it offers network-level blocking, optional blocking features developed by Comcast, and third-party blocking applications.[118] Between March 2020 and

[105] *Id*.

[106] *Id*.

[107] *Id.* at 1.

[108] *Id*.

[109] *Id.* at 2.

[110] *Id*.

[111] *Id*.

[112] *Id*.

[113] *Id*.

[114] *Id*.

[115] *Id*.

[116] *Id*. at 3.

[117] *Id*.

[118] Letter from Charles Herrin, President, Technology, Product, and Xperience, Comcast Cable, to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 1 (Apr. 30, 2021) (Comcast Letter).

March 2021, these tools collectively blocked more than 2.3 billion inbound call attempts to Comcast customers (including over one billion blocked calls at the network level using edge blocking).[119] At the network level, Comcast uses specific robocall mitigation techniques; for Xfinity Voice, Business Voice Mobility, VoiceEdge Select, Business VoiceEdge, and Business Voice Trunking customers, Comcast has configured edge devices on its voice network to block calls appearing to originate from numbers on the industry DNO list and from invalid or unallocated telephone numbers, at no additional charge.[120] Comcast estimates that, between March 2020 and March 2021, it blocked more than 1 billion illegal and fraudulent robocall attempts at the network level using this edge blocking technique (i.e., network-level blocking).[121]

40. Comcast explains that it automatically rejects calls from invalid numbers, numbers on the DNO list, and numbers otherwise identified as problematic by the Industry Traceback Group (ITG); rejects inbound calls from numbers demonstrating poor call completion, short call duration, or excessive attempts to disconnected numbers; and rejects inbound calls from numbers exhibiting nuisance calling patterns by utilizing a calculated "robo score."[122] According to Comcast, "robo scoring" is an algorithmic analysis based on call statistics, including average call duration and unanswered rate, that scores a particular inbound telephone number on a scale from -10 to +10; a higher score means that it is more likely the calling pattern indicates nuisance calling.[123] On average, these efforts result in the blocking of between 1.5 billion and 2.5 billion unwanted or fraudulent call attempts per month.[124] Comcast also is developing and deploying new technology that is more customizable, treating calls based on dynamic considerations, and using machine-learning capabilities to enhance Comcast's ability to identify problematic traffic.[125]

41. Comcast also has been expanding call authentication capabilities, including the recent rollout of Verified Caller ID functionality, has implemented substantial safeguards in its wholesale business, and has taken active measures to avoid inadvertent blocking of emergency calls.[126]

42. Comcast offers additional robocall mitigation tools to customers at no additional charge; for residential Xfinity Voice subscribers and business customers, Comcast offers, on a default opt-out basis, Anonymous Call Rejection, which automatically rejects calls where the caller has chosen to prevent the display of the caller's name and number.[127] Comcast estimates that, between March 2020 and March 2021, this tool blocked nearly 1.15 billion unwanted call attempts.[128]

43. Comcast also offers residential Xfinity Voice and certain business customers a more tailored robocall mitigation tool called Selective Call Rejection, or Call Screening, on an opt-in basis.[129] This free tool enables a customer to create a list of up to 25 telephone numbers that, instead of getting through to the customer's phone, will receive an announcement stating that the customer is not

[119] Comcast Letter at 1-2.

[120] *Id.* at 2.

[121] *Id*.

[122] *Id.* at 4.

[123] *Id*. at 4 & n.9.

[124] *Id*. at 4.

[125] *Id*.

[126] *Id*. at 1.

[127] *Id.* at 2.

[128] *Id*.

[129] *Id*.

available.[130] Comcast estimates that this tool blocked over 58 million unwanted call attempts bound for Comcast customers between March 2020 and March 2021.[131] Comcast is also testing a nuisance call treatment tool that will be free to Xfinity Voice customers and should be launched in the second half of 2021, that uses Comcast tools and third-party analytics to rank incoming calls as "High," "Medium," or "Low" likelihood of being spam calls.[132] Comcast customers will choose how they want to treat these calls—allowing them to be completed, sending the calls to voicemail, or blocking the calls.[133] In addition, Comcast customers will be able to change their settings and have visibility into their call logs and voicemail records through the Xfinity Connect web portal.[134]

44. Comcast also enables its customers to identify and block unwanted robocalls by using free third-party applications on an opt-in basis, such as Nomorobo, a cloud-based service that can be configured to block various types of robocalls.[135] Comcast estimates that, between March 2020 and March 2021, this service successfully blocked more than 105 million call attempts bound for subscribers who had activated the service.[136]

45. In December 2020, Comcast activated a free call filtering functionality for Xfinity Mobile customers, which displays "Possible Spam" on the customer's device for inbound calls identified as potentially fraudulent.[137] Moreover, all Xfinity Mobile customers using an iOS device have incoming likely spam calls rerouted to voicemail by default, as an opt-out feature.[138]

46. In addition, Comcast has implemented end-to-end call authentication capability based on the STIR/SHAKEN protocol.[139] Comcast is continuing to sign virtually all calls originating from Comcast residential voice customers and small- and medium-sized business voice customers; as of March 2021, approximately 30% of all calls originating from other providers and bound for such customers are signed and verified.[140] Comcast also has a new caller ID verification tool for all residential and small- and medium-sized business customers that provides customers with more information about the level of trust associated with a particular call by displaying the word "Verified" (or the letter "V") any time the caller's voice provider has confirmed that the call is coming from a legitimate telephone number.[141] Comcast displays this verification on the phone screen, on the television screen (for customers with Comcast's latest set-top box), on the customer's call log, and on voicemail records.[142] This display is available only for calls coming from providers sharing STIR/SHAKEN authentication information with Comcast.[143]

---

[130] *Id*.

[131] *Id*.

[132] *Id*.

[133] *Id*.

[134] *Id*.

[135] *Id*.

[136] *Id*.

[137] *Id.* at 3.

[138] *Id*.

[139] *Id*.

[140] *Id*.

[141] *Id.* at 3-4.

[142] *Id*.

[143] *Id*.

47. Comcast's wholesale business has taken various actions to prevent potentially harmful traffic from transiting Comcast's network, such as prohibiting its wholesale customers from sending significant volumes of short-duration traffic and expressly requiring cooperation with traceback requests and registration in the Robocall Mitigation Database.[144] If problematic traffic is detected, Comcast provides warnings, limits capacity, and even terminates services.[145]

48. *Cox Communications, Inc. (Cox)*. Cox provides network-based call blocking (Edge Blocking) to block DNO, invalid, and unallocated telephone numbers.[146] The Cox network actively identifies and blocks calls displaying DNO telephone numbers and inbound calls purportedly originating from 10-digit numbers that are not valid North American Numbering Plan numbers.[147] Cox completed the migration of its residential customers to an all-IP STIR/SHAKEN-enabled network by March 1, 2020.[148] This will allow Cox to develop and offer new call-blocking tools to its residential customers.[149]

49. The primary call-blocking tool currently available to Cox's residential customers is Nomorobo, a third-party service, which automatically identifies and blocks potentially unwanted and illegal calls using Simultaneous Ring technology.[150] Nomorobo sends an intercept message to the calling party when calls are blocked.[151] There is no cost to customers to use Nomorobo, and Cox automatically provides the Simultaneous Ring feature to customers for free, which then allows customers to sign up for the third-party service and activate the feature.[152] Five percent of Cox's residential customers have completed the sign-up process for Nomorobo's service.[153]

50. Cox also offers its residential customers other call blocking features at no additional charge, such as Anonymous Call Rejection, which allows customers to reject calls from callers who block their caller ID from displaying, and Selective Call Rejection, which allows customers to create a personal blacklist of telephone numbers that will be blocked or rejected.[154] Approximately 97% of customers with Anonymous Call Rejection have activated the feature, and fewer than 5% of customers use the Selective Call Rejection feature.[155] Calling parties receive an intercept message when their calls are blocked by Anonymous Call Rejection or Selective Call Rejection.[156]

51. Cox blocks 10.2% of incoming call attempts to residential customers through a combination of Edge Blocking, Anonymous Call Rejection, Nomorobo, and Selective Call Rejection.[157]

---

[144] *Id.* at 4.

[145] *Id.*

[146] Cox Comments at 2-3.

[147] *Id.* at 3.

[148] *Id.* at 1.

[149] *Id.*

[150] *Id.*

[151] *Id.* at 1-2.

[152] *Id.* at 2.

[153] *Id.*

[154] *Id.*

[155] *Id.*

[156] *Id.*

[157] *Id.* at 3.

Edge Blocking accounts for 72% of these call attempts, followed by Anonymous Call Rejection which represents an additional 16% of blocked calls.[158]

52. *Frontier Communications (Frontier).* Frontier explains that it has deployed STIR/SHAKEN on its IP network and has begun exchanging authenticated STIR/SHAKEN traffic.[159] Frontier conducts network-level call-blocking for numbers on the DNO list.[160] Frontier also offers several opt-in call-blocking tools across both its IP and TDM networks, free of charge, including anonymous call rejection, selective call rejection, and selective call acceptance; it also allows subscribers to use third-party applications like Nomorobo.[161] Additionally, Frontier has deployed an advanced caller ID alert system using Neustar Robocall Mitigation technology, to indicate whether a call is legitimate by displaying a "Potential Spam" alert on the call recipient's device.[162]

53. *INCOMPAS.* INCOMPAS[163] states that its members report that some carriers or third-party analytics companies are diverting traffic to dead air or fake voicemail.[164] These originating voice service providers have subsequently seen a significant rise in customer complaints, with the volume of complaints increasing noticeably after the Commission adopted safe harbors for call blocking.[165] In addition, INCOMPAS states there are concerns that call blocking, call diversion, and call rating could impair online security efforts given the potential for multi-factor authentication calls to be blocked or diverted under the misperception that they are illegal robocalls, or erroneously characterized as "spam likely" and thus not answered by the recipient.[166] INCOMPAS also observes that, according to its members, the protocol around SIP codes is still a work in progress as the codes are not being translated correctly and the response to some SIP codes has been inconsistent between carriers.[167]

54. *Lumen Technologies (Lumen) (formerly CenturyLink).*[168] Lumen explains that it monitors its networks for mass calling events and coordinates with other major providers, the ITG, trusted third parties, and key federal agencies to address and mitigate obviously fraudulent calls at the network level.[169] In coordination with the ITG, Lumen performs DNO blocking of government impersonation

[158] *Id.*

[159] Letter from Kenneth Mason, Senior Vice President, Federal Regulatory and Government Affairs, Frontier Communications, to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 1 (Apr. 30, 2021) (Frontier Letter).

[160] Frontier Letter at 1.

[161] *Id. See* Frontier, *How to Block Telemarketing Calls*, https://frontier.com/helpcenter/categories/phone/calling-features/block-telemarketing-calls (last visited June 15, 2021).

[162] Frontier Letter at 2.

[163] INCOMPAS (the Internet and Competitive Networks Association, formerly named COMPTEL), is a trade association representing internet, streaming, communications, and technology companies.

[164] INCOMPAS Comments at 2.

[165] *Id.*

[166] *Id.* at 3.

[167] *Id.* at 4. The Commission has adopted requirements for terminating voice service providers to transmit certain SIP or ISUP codes when calls are blocked, effective January 1, 2022. *See Call Blocking Fourth Report and Order*, 35 FCC Rcd at 155239-242, paras. 52-61.

[168] On Sept. 14, 2020, CenturyLink rebranded as Lumen Technologies, *see* News Details, "*CenturyLink Transforms, Rebrands as Lumen*," (Sept. 14, 2020), https://ir.centurylink.com/news/news-details/2020/CenturyLink-Transforms-Rebrands-as-Lumen/default.aspx.

[169] Letter from David C. Bartlett, Vice President, Federal Government Relations, Lumen Technologies, to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 2 (Apr. 30, 2021) (Lumen Letter).

calls.[170] Lumen also blocks "call back" Direct Inward Dial (DID) numbers used by such scams, and may block calls from numbers associated with mass robocalling scam campaigns as identified by a trusted third party.[171] Lumen may also conduct additional network-level blocking in response to "cease-and-desist" letters issued by the Commission to the extent the recipients of those letters fail to undertake the directed remedial measures.[172]

55. Lumen explains that it has been implementing STIR/SHAKEN call authentication technology on the IP portions of its network in order to meet the June 30, 2021 implementation deadline; the company is signing calls traversing its IP networks and expanding that capability to facilitate traceback and enable consumers to have greater confidence that calling parties are who they say they are.[173] Lumen has also participated in industry efforts to bring the benefits of call authentication technology to non-IP networks.[174] In 2020, Lumen agreed to lead the Non-IP Call Authentication Task Force established by Alliance for Telecommunications Industry Solutions (ATIS) which will complement the work already being addressed by the Internet Protocol Network-to-Network Interconnection (IP-NNI) Task Force to address challenges with call authentication on TDM networks and identify viable alternatives for TDM call-authentication functionality.[175]

56. In addition to network-level blocking, Lumen continues to make Nomorobo available to its consumer VoIP customers.[176] For TDM customers, Lumen continues to offer several call-screening tools on an opt-in basis to prevent illegal robocallers from harassing end users: the No Solicitation service that plays an automated message asking solicitors to hang up and tells callers to press a specific key in order to reach the end user, and the Security Screen feature that requires callers from blocked, unidentified, toll-free, or long-distance numbers to enter their 10-digit telephone number before their call will connect to the end user.[177] The No Solicitation and Security Screen features disrupt the operation of automated robocalling platforms and can significantly reduce the number of unwanted calls that are reaching and disturbing customers.[178]

57. Lumen states that it also offers, on an opt-in basis, Caller ID with Privacy+, which prompts calling parties lacking Caller ID information to provide a name in order to complete their calls; Anonymous Call Rejection, which enables customers to choose to block calls from "private" or anonymous numbers; and Call Rejection and Enhanced Call Rejection, which enable customers to choose to block calls from specific numbers.[179] Other opt-in features, such as Do Not Disturb and Call Curfew are designed to enable customers to choose to block all incoming calls during specified nighttime hours.[180] Lumen continues to evaluate new data analytics tools for use in conjunction with and as a complement to STIR/SHAKEN.[181] Lumen engineers are also evaluating options to supplement Caller ID

[170] Lumen Letter at 2.

[171] *Id.*

[172] *Id.*

[173] *Id.* at 1.

[174] *Id.*

[175] *Id.* at 1-2.

[176] *Id.* at 3.

[177] *Id.*

[178] *Id. See* Lumen, *Lumen Help, Blocking Calls from Anonymous Callers*, https://www.lumen.com/help/en-us/voip/business-communicator/blocking-calls-from-anonymous-callers.html (last visited June 15, 2021).

[179] Lumen Letter at 3.

[180] *Id.*

displays so they reflect additional verification information to provide end users enhanced screening capabilities.[182]

58. *NCTA—The Internet and Television Association (NCTA).* NCTA explains that its member cable operators share the Commission's and the public's desire to put a stop to illegal and unwanted robocalls.[183] Cable operators have been involved in establishing the STIR/SHAKEN call authentication framework and governance system.[184] Charter, Cox, and Comcast have implemented the STIR/SHAKEN call authentication framework on their networks and were granted exemptions for demonstrating substantial early progress toward full deployment.[185] NCTA states that the cable industry has participated in other industry and Commission efforts to combat robocalls, including the Hospital Robocall Protection Group, the Voice Service Providers Working Group chaired by Charter, and the ITG, for which Comcast, Charter, and Cox serve on the Executive Committee.[186]

59. Within their own companies, NCTA's members have deployed a variety of additional tools, at no charge to consumers, to fight illegal and unwanted robocalls, such as access to Nomorobo's call blocking service and Call Guard, offered by Charter on an opt-out basis.[187] NCTA states that Comcast, Cox, and Charter offer their subscribers the ability to block specific callers and callers who prevent their Caller ID from displaying.[188] Cable operators also block harmful robocalls at the network level without consumer opt-in or opt-out, such as network-level blocking of calls that appear to originate from numbers on the industry DNO list or from invalid or unallocated numbers.[189] Comcast and Charter also offer free call blocking for their mobile subscribers.[190] Smaller cable carriers Midco, Mediacom, and GCI also offer their customers call blocking.[191]

60. *TDS Telecom.* TDS Telecom states that it uses Call Guardian Authentication Hub by Transaction Network Services (TNS) and Metaswitch (a Microsoft company) to provide a network-level tool to identify robocalls.[192] This tool is analytics-based and uses real-time call events and crowd sourced data to create reputation profiles and block illegal robocalls.[193] This network-level tool works on the IP and TDM portions of the network to maximize call blocking for TDS Telecom customers.[194] In March 2021, over 24 million calls were analyzed and approximately 10% were identified as high risk and

(Continued from previous page)

[181] *Id.*

[182] *Id.*

[183] NCTA Comments at 1.

[184] *Id.* at 1-2.

[185] *Id.* at 2.

[186] *Id.*

[187] *Id.*

[188] *Id.*

[189] *Id.* at 3.

[190] *Id.*

[191] *Id.*

[192] Letter from Ken Paker and Andrew Petersen, TDS Telecommunications LLC, to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 1 (Apr. 30, 2021) (TDS Telecom Letter).

[193] TDS Telecom Letter at 1.

[194] *Id.*

blocked, including those from invalid numbers and on the DNO list.[195] Implementation of this service is in progress and should be completed by June 2021.[196] This call blocking service is opt-out.[197]

61. *T-Mobile*. T-Mobile explains that, in July 2020, it began offering Scam Shield, which includes caller ID and several features at no additional cost. The first feature is Scam ID, offered by default; all customers get a "Scam Likely" alert for suspect calls. Another is Scam Block, which blocks calls identified as "Scam Likely" at the network level. Number change provides a new number for customers who have become spam targets, while T-Mobile PROXY provides a second number for some customers.[198] T-Mobile customers can control the call blocking features through the free Scam Shield application, which also offers the option of premium services like the ability to send entire categories of unwanted calls to voicemail, create "always block" lists, and set up voicemail-to-text services.[199] These additional features are included for T-Mobile primary account holders with Magenta MAX plans, and cost $4.00 per month per line for all other subscribers.[200] Roughly 80 million subscribers use Scam Shield, up nearly 13 million since June 1, 2020.[201] T-Mobile states that its call identification and blocking tools have identified over 33 billion calls as scams and blocked roughly 9 billion of those scam calls to date.[202]

62. *UScellular*. UScellular offers call blocking through third-party analytics provider TNS' Call Guardian device application for Android and iOS-based devices.[203] Call Guardian provides customers with the ability to know they are receiving a potentially fraudulent call and the capability to block the call at their device.[204] UScellular's VoLTE-enabled subscriber base, over 85% of UScellular subscribers, has free network-level call analytics tools and blocking.[205] In addition, the Call Guardian app is being used by approximately 9% of UScellular subscribers.[206] The basic version of Call Guardian is free; the premium level subscription allows users to block certain types of calls at their discretion and is free to all UScellular subscribers enrolled in the Top Tier Postpaid Unlimited plans—otherwise, the monthly fee is $3.99.[207]

63. The VoLTE network analytics block calls that are identified as highest risk. The consumer can opt out of this protection.[208] The premium device app allows the customer to opt in to blocking high and medium risk calls.[209] The VoLTE network-based call-blocking tool, TNS Call

---

[195] *Id.* at 2.

[196] *Id*.

[197] *Id*.

[198] Letter from Michele K. Thomas, Vice President, Regulatory Affairs, T-Mobile USA, Inc., to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 2 (Apr. 30, 2021) (T-Mobile Letter).

[199] T-Mobile Letter at 3.

[200] *Id*.

[201] *Id*.

[202] *Id.* at 4.

[203] Letter from Grant B. Spellmeyer, Vice President, Federal Affairs and Public Policy, United States Cellular Corp., to Marlene H. Dortch, Secretary, FCC at 1 (Apr. 30, 2021) (UScellular Letter).

[204] UScellular Letter at 1.

[205] *Id*.

[206] *Id*.

[207] *Id*.

[208] *Id.* at 2.

Guardian, blocks calls with improperly formatted calling numbers, or numbers that have been identified as DNO.[210] The Call Guardian analytics use calling number history, STIR/SHAKEN verification status, and other call related information.[211] Callers blocked by the network receive immediate notification.[212]

64. UScellular blocked approximately 45 million robocalls at the network level during the first quarter of 2021 using the call analytics from TNS.[213] Although UScellular does not offer white list blocking,[214] certain handset manufacturers, including Apple, offer the ability to do so, and customers can block individual numbers on their devices or through the Call Guardian app.[215]

65. *USTelecom—The Broadband Association (USTelecom)*. USTelecom[216] established the Industry Traceback Group (ITG) in 2015, and the ITG has played a central role in the battle against illegal robocalls.[217] In 2020, the ITG received 75 subpoenas and civil investigative demands, up 275% from 2019; conducted approximately 215 tracebacks per month, up 115% from 2019 and 975% from 2018; initiated more than 2,500 tracebacks;[218] and supported nearly one dozen enforcement actions involving nine distinct federal and state enforcement agencies, targeting nearly 50 individuals and entities.[219]

66. Last year, USTelecom established a working group, co-chaired by representatives of AT&T and Twilio, to assess and develop consensus best practices for blocking and labeling transparency, redress, and other caller protections.[220] This working group has developed an easy-to-find resource for callers seeking call labeling and blocking points of contact at http://www.ustelecom.org/call-redress and has asked the IP-NNI Task Force to review the technical feasibility and potential best practices of notification for blocking and labeling.[221] Currently, the working group is seeking to develop consensus on redress best practices for providers and their analytics partners to address inadvertent blocking or mislabeling of legitimate wanted calls when they arise.[222]

67. *Verizon*. Verizon explains that, at the network level, it has blocked hundreds of millions of calls on an across-the-board (i.e., not opt-in or opt-out) basis where the calling party number is invalid or unassigned, or where the person to whom the number was assigned has authorized the block.[223]

(Continued from previous page)

[209] *Id*.

[210] *Id*.

[211] *Id*.

[212] *Id*.

[213] *Id.* at 3.

[214] Voice service providers may offer white list programs on an opt-in basis, i.e., blocking calls from numbers not in a consumer's contacts list. *2019 Call Blocking Declaratory Ruling*, 34 FCC Rcd at 4890-91, paras. 43-46.

[215] UScellular Letter at 3.

[216] USTelecom is a trade association representing service providers and suppliers for the communications industry that provide broadband, voice, data, and video services over wireline and wireless networks.

[217] USTelecom Comments at 1. The ITG has been selected as the single consortium. *See ITG Consortium Order*, 35 FCC Rcd 7886.

[218] Each call traced back may be part of a large calling campaign that could have placed millions of calls.

[219] USTelecom Comments at 1-2. For a more detailed description of the traceback process, *see* Industry Traceback Group, *Combatting Illegal Robocalls*, https://www.ustelecom.org/research/combatting-illegal-robocalls/ (last visited June 15, 2021).

[220] USTelecom Comments at 2.

[221] *Id.*

[222] *Id.*

Verizon also blocks additional illegal robocalls using advanced data analytics, pattern recognition, and machine learning with human oversight, such as one-ring scam calls (and also blocks the consumer's call-back).[224]

68. For Verizon wireless subscribers, the number of subscribers using the free opt-out Call Filter blocking service increased from 50 million in June 2020 to more than 75 million in April 2021.[225] Verizon offers a free version of Call Filter and a premium version called Call Filter Plus.[226] For all Call Filter and Call Filter Plus customers, Verizon automatically blocks by default all calls identified as potential fraud.[227] Verizon wireless customers can leave in place the default (which blocks only high risk, potential fraud calls) or they can adjust the blocking to include medium risk (potential spam, which often involves callers disguising their numbers) and/or lower risk (potentially unwanted) calls.[228] Verizon Call Filter takes into consideration a call's STIR/SHAKEN verification results as one component of the more holistic real-time analysis to determine whether to block or label a call.[229]

69. Starting in July 2020, Verizon made network-based enhancements to block more unwanted calls, allow customers to choose whether to terminate the call before it reaches the device or forward it to voicemail, and provide a way for customers to manage their block settings and view lists of blocked calls.[230] Verizon sends calls blocked by Call Filter to voicemail and identifies those voicemails as potential spam (unless the customer changes their settings to instead terminate the call before it reaches the device, which is a setting available for certain devices only).[231] Wireless customers can see a log of blocked calls within the Call Filter app or their My Verizon portal.[232]

70. In September 2020, Verizon and Apple provided a new Silence Junk Callers feature to Verizon Call Filter customers with iPhones.[233] That feature is enabled by default to forward to voicemail all high and medium-risk spam calls.[234] With Call Filter, customers can screen incoming spam calls, block (send directly to voicemail) spam numbers by risk level, and report numbers as spam; numbers considered risky are labeled as "Potential Spam."[235] With Call Filter Plus, customers receive all the features of Call Filter and also can see the caller's name for unknown numbers, create a custom block list,

(Continued from previous page)

[223] Letter from Christopher D. Oatway, Associate General Counsel, Federal Regulatory and Legal Affairs, Verizon Communications Inc., to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 3 (Apr. 30, 2021) (Verizon Letter).

[224] Verizon Letter at 3.

[225] *Id.* at 2.

[226] *Id*. *See* Verizon, *Helping Our Customers Block Robocalls*, https://www.verizon.com/about/responsibility/robocalls (last visited June 15, 2021); Verizon, *Call Filter, Answer with Confidence*, https://www.verizon.com/solutions-and-services/call-filter/ (last visited June 15, 2021).

[227] Verizon Letter at 2.

[228] *Id.* at 3.

[229] *Id.* at 7.

[230] *Id.* at 2.

[231] *Id.* at 6.

[232] *Id.* at 6-7.

[233] *Id.* at 2.

[234] *Id*.

[235] *Id*.

view the risk-level of incoming calls, and use a spam lookup feature to see if a number has already been identified as spam.[236]

71. All Verizon landline customers (copper and fiber) have access to free Spam Alerts, which is a robocall-labeling service for all customers with caller ID; it displays "SPAM?" before a caller's name if the calling number matches certain criteria designed to identify likely spam.[237] Verizon's Fios Digital Voice customers can receive the free Nomorobo simultaneous ring feature.[238] Verizon intends to provide call blocking tools on an opt-out basis for Fios Digital Voice customers later this year, which will automatically block calls identified as potential fraud; the customer will be able to review blocked calls in their call log.[239]

72. Verizon explains that the pandemic initiated a wave of COVID-19-related fraudulent robocalls, including ones purporting to offer free testing or free personal protective equipment; Verizon passed to the ITG numerous leads about illegal COVID-19 scams based on calls to numbers identified by its honeypot (i.e., a decoy to lure attacks), so that law enforcement could take appropriate action.[240]

73. Verizon observes that robocallers continuously deploy new tactics, such as using large pools of non-spoofed numbers apparently assigned to them and inserting messages into nonconsenting consumers' voice mailboxes without the calls causing the consumers' devices to ring.[241] Verizon notes that previously robocallers would exploit the fact that certain voicemail systems provided portals that permitted callers to automatically record and send ringless voicemails.[242] Robocallers would use robots to navigate those voicemail portal menus in order to send large numbers of prerecorded messages directly into nonconsenting consumers' voice mailboxes.[243] After Verizon, and most other service providers, shut off robocallers' ability to navigate voicemail systems to leave ringless voicemails, the robocallers now send two nearly-simultaneous calls to a consumer's line; the first call ties up the line, which causes the next one to go directly into the customer's voicemail.[244] The robocaller then deposits the prerecorded ringless voicemail into millions of consumers' voice mailboxes.[245] Verizon is developing countermeasures to protect customers and networks from this new technique.[246]

74. *Vonage*. Vonage explains that it offers its Spam Shield[247] service to business customers, which identifies suspected spam within the caller ID to allow the called party to decline the call; since August 2020, Vonage offers an equivalent service to residential customers.[248] Previously, Spam Shield

---

[236] *Id.*

[237] *Id.* at 3.

[238] *Id.*

[239] *Id.*

[240] *Id.* at 4.

[241] *Id.* at 1.

[242] *Id.* at 5.

[243] *Id.*

[244] *Id.* at 6.

[245] *Id.*

[246] *Id.*

[247] Vonage, *Spam Shield*, https://www.vonage.com/unified-communications/features/spam-shield/ (last visited June 15, 2021).

[248] Letter from Randy Rutherford, Chief Legal Officer, Vonage Holdings Corp., to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 1 (Apr. 28, 2021) (Vonage Letter). *See* Vonage, *Vonage*

(continued….)

was provided by Nomorobo; however, now Spam Shield is based on Vonage's own internally developed solution, in reliance on Neustar data.[249] Since August 2020, Vonage offers Spam Shield at no additional charge for both business and residential subscribers.[250] Vonage plans to enhance its Spam Shield feature for business customers that opt in, to send all incoming calls that have been identified as likely spam to voicemail.[251] Vonage also offers its business and residential customers further call-blocking options based on the caller ID of incoming calls;[252] anonymous call blocking of calls where caller ID information is not displayed;[253] selective call blocking of calls based on specific numbers;[254] and do not disturb to block all incoming calls temporarily.[255]

B. Third-party Analytics Companies' Blocking Services

75. Several third-party analytics companies that provide blocking services submitted information about their services, including how they have updated their blocking services since the First Call Blocking Report.

76. *First Orion.* T-Mobile provides Scam ID and Scam Block services through First Orion's data analytics platform and services.[256] First Orion also supports certain components of T-Mobile's Scam Shield offering, which, among other consumer protection services, enables subscribers to activate and manage scam labeling and blocking features.[257] First Orion provides, on an opt-in basis, both free and fee-based applications under the PrivacyStar brand and works with Tracfone and Boost Mobile to offer application-based call treatment tools for their subscribers.[258] These PrivacyStar applications offer features such as Phone Number Lookup, free of charge, and have subscription fees ranging from $0.99 to $3.99 for additional features.[259] In July 2020, T-Mobile announced its expanded Scam Shield service for its customers including Scam ID, Scam Block, free opt-in Caller ID with Name also provided by First Orion, as well as a number of other First Orion services.[260]

77. First Orion recently implemented enhanced analytics approaches to address "ultra-low volume" scamming, an even bigger challenge than the "traditional" high volume, random dialing

(Continued from previous page)
Residential Support, *Detect Spam and Robocalls Email*, https://support.vonage.com/articles/answer/Detect-Spam-and-Robocalls-Email-Res (last visited June 15, 2021).

[249] Vonage Letter at 1.

[250] *Id.*

[251] *Id.*

[252] *Id.* at 2.

[253] Vonage, *Vonage Residential Support*, *Anonymous Call Block*, https://support.vonage.com/articles/answer/Anonymous-Call-Block-951 (last visited June 15, 2021).

[254] Vonage, *Vonage Residential Support*, *Selective Call Block*, https://support.vonage.com/articles/Answer/Selective-Call-Block-13990 (last visited June 15, 2021).

[255] Vonage, *Vonage Residential Support*, *Do Not Disturb On and Off*, https://support.vonage.com/articles/answer/Turn-Do-Not-Disturb-On-and-Off-9723 (last visited June 15, 2021).

[256] Letter from Charles Morgan, CEO and Chairman, First Orion Corp. to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 1 (Apr. 30, 2021) (First Orion Letter).

[257] First Orion Letter at 1.

[258] *Id.*

[259] *Id.*

[260] *Id.* at 2.

approach many scammers continue to use.[261] First Orion is constantly updating its analytics capabilities to address changes in scammer tactics.[262]

78. First Orion's Scam ID, which is a labeling service, is available free of charge on an opt-out basis to T-Mobile and Metro by T-Mobile subscribers regardless of rate plan or device.[263] With First Orion's Scam Block, subscribers may opt in to have these calls blocked rather than labeled.[264] Over 80 million T-Mobile subscribers are protected by First Orion from scam calls either by labeling or blocking.[265] First Orion currently identifies over 300 million scam calls per week, with a false positive rate of a fraction of 1%.[266] The Scam Shield mobile app, available for iOS and Android, is also free, and offers additional features for a fee.[267] Scam ID (opt-out) and Scam Block (opt-in) identify and block invalid numbers and Do Not Originate numbers.[268] Calls identified that analytics identify as fraudulent are labeled "Scam Likely" as part of the opt-out Scam ID service.[269] The subscriber can control whether to block these or to just have the calls labeled as Scam Likely. With Scam Shield app, the subscriber can elect to also have other categories of calls treated.[270] Calls labeled via Scam ID are displayed in the subscriber's native call log and also in the Scam Shield app.[271] Calls blocked due to invalid number status and calls blocked for subscribers who have opted in for Scam Block can access the blocked call information in the Scam Shield app.[272]

79. *Hiya.* Hiya offers call blocking and labeling services through AT&T Call Protect, Samsung Smart Call, and the Hiya app, as well as through new partnerships with Cricket Wireless and Telenor Norway.[273] Hiya Protect, provided at the carrier level without charge to end users, protects consumers from spam and fraud calls, and without blocking wanted callers.[274]

80. In 2020, Hiya served more than 150 million monthly active users globally, approximately 50 million more users than in 2019; it also processed more than 150 billion calls.[275] Hiya alerted users of more than 7.5 billion incoming spam calls and helped block nearly 1.2 billion of them.[276] Hiya is integrated into the AT&T network and provides AT&T Call Protect, which enables AT&T to automatically block known fraud calls from reaching their customers and provides spam labels for known spam calls, at no additional charge to AT&T subscribers.[277] Hiya also powers Samsung Smart Call,

[261] *Id.*

[262] *Id.*

[263] *Id.*

[264] *Id.*

[265] *Id.*

[266] *Id.* at 3.

[267] *Id.* at 2.

[268] *Id.* at 3.

[269] *Id.*

[270] *Id.*

[271] *Id.*

[272] *Id.*

[273] Letter from Alex Algard, CEO, Hiya, to Mika Savir, Consumer and Governmental Affairs Bureau, FCC at 1 (Apr. 30, 2021) (Hiya Letter).

[274] Hiya Letter at 2.

[275] *Id.*

[276] *Id.*

which flags spam calls, automatically blocks known fraud calls, and provides caller ID to Samsung customers, at no additional charge.[278]

81. The Hiya app, which is available for download for iOS and Android devices as a free or premium offering, provides advanced controls over incoming-call filtering.[279] The free version offers call blocking and filtering; the premium version includes enhanced caller ID features and functionality.[280] Users of these apps select whether to be warned of fraudulent calls or to block calls flagged as fraud, and separately to be notified of any calls considered spam, such as surveys, telemarketing, and debt collection calls.[281]

82. *Innovative Systems.* Innovative Systems provides a telemarketer call screening and blocking tool for landlines called APMAX Terminating Call Manager (TCM) to the rural telecommunications market.[282] This service is currently installed at over 207 rural landline provider locations.[283] Only a small percentage of rural service providers offer this to their consumers at no cost.[284] In a survey of 60 Innovative Systems service providers, the call screening service was available to 505,303 consumers, but only 13,183 had the service activated on their phone lines, probably due to the opt-in and cost requirements.[285] The monthly fee for consumers ranged from $2 to $5 per month to have the call screening tool installed on their landlines.[286]

83. Innovative Systems contends that the effectiveness of an opt-out, no-cost call blocking solution is evidenced by a data report from Peoples Telecom in Quitman, Texas, where during the period of October 2020, to April 2021, the company's 5,874 landlines received 789,725 calls from outside their exchange territory that received the challenge announcement, "The number you have reached does not accept calls from telemarketers. If you are a telemarketer, please add this number to your do not call list and hang up now. Otherwise, press 1 or stay on the line."[287] Out of this number, 660,814 calls were tabulated as disconnects, meaning they did not make a response to the challenge.[288] Most of the disconnected calls were robocalls and 727,095 of the calls were known telemarketers.[289]

84. At the network level, Innovative Systems service compares incoming trunk group calls against a local NPA-NXX allowed list.[290] Any numbers that appear to be local numbers, but which come from outside the local network on a trunk group, i.e., spoofed calls, will be challenged unless they are already on an allowed list.[291] Callers that dial 1 to pass through a challenge announcement will be placed

(Continued from previous page)

[277] *Id.*

[278] *Id.*

[279] *Id.*

[280] *Id.*

[281] *Id.*

[282] Innovative Systems Comments at 1.

[283] *Id.*

[284] *Id.*

[285] *Id.*

[286] *Id.*

[287] *Id.*

[288] *Id.*

[289] *Id.* at 2.

[290] *Id.*

on the allowed list.[292] At the device level, the Innovative Systems service challenges calls by comparing them against a known-caller number list for each subscriber.[293] Calls that are received by an unknown party or that are not on the known caller list are intercepted and will hear a challenge announcement.[294] Calls from numbers on a blocked caller list will hear a blocking announcement.[295]

85. Innovative Systems has tabulated reports for 2020 from 25 voice providers with its service deployed on 11,233 landlines; those phone numbers received over 3.6 million suspected spam calls and over 1.6 million known telemarketer and robocall numbers were thwarted.[296] Only 118,068 of calls challenged by the service activated or pressed a dial-through digit or waited for their call to complete.[297]

86. *Nomorobo.* Nomorobo explains that its mobile and landline service is used by over two million phone lines daily,[298] which reflects a growth in the number of users since June 2020.[299] Nomorobo landline service is free; the mobile product has a 14-day free trial and then costs $1.99/month or $19.99/year.[300] Nomorobo blocks both illegal and unwanted calls, whether they are automatically or manually dialed, and malicious SMS text messages.[301] Nomorobo (for VoIP landlines) uses a feature known as Simultaneous Ring.[302] When simultaneous ring is enabled, the subscriber's phone will ring on more than one number at the same time.[303] The first device to pick it up gets the call—when the Nomorobo number is enabled as a simultaneous ring number, it is the first number to screen the call.[304] The call goes through to the subscriber's number if it is a legitimate call.[305] If the call is an illegal robocall, Nomorobo intercepts the call and hangs up.[306] On landlines, consumers hear a single ring and see the caller ID before the call is intercepted.[307] On mobile phones, if the consumer chooses "Identify," an alert is displayed.[308] If the consumer chooses "Blocked," they receive an alert only if the robocaller leaves a voicemail.[309] In both cases, in the "Recents" and "Voicemail" lists, calls are identified as

(Continued from previous page)

[291] *Id.*

[292] *Id.* at 3.

[293] *Id.*

[294] *Id.*

[295] *Id.*

[296] *Id.*

[297] *Id.*

[298] Letter from Aaron Foss, President and CFO, Telephone Science Corp. d/b/a Nomorobo to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 1 (Apr. 30, 2021) (Nomorobo Letter).

[299] Nomorobo Letter at 1.

[300] *Id.*; Nomorobo, https://www.nomorobo.com/ (last visited June 15, 2021).

[301] Nomorobo Letter at 1.

[302] Nomorobo, *How Does It Work on Landlines?*, https://nomorobo.zendesk.com/hc/en-us/articles/200536477-How-does-it-work-on-Landlines- (last visited June 15, 2021).

[303] *Id.*

[304] *Id.*

[305] *Id.*

[306] *Id.*

[307] Nomorobo Letter at 1.

[308] *Id.*

"Robocaller."[310] Nomorobo's landline service presents blocked callers with a voice CAPTCHA;[311] Nomorobo plans on returning the SIP rejection code on all blocked calls this year.[312]

87. *Teltech Systems, Inc. (Teltech or RoboKiller).* Teltech Systems explains that it creates and offers RoboKiller, a mobile application that automatically blocks spam calls, and other related products.[313] RoboKiller won the FTC's 2015 Robocalls: Humanity Strikes Back contest.[314] RoboKiller uses a proprietary algorithm powered by "audio-fingerprinting" and audio analysis, machine learning, and user feedback to block unwanted calls.[315] In addition to the RoboKiller mobile application, Teltech also offers the Call Confidence API for business and telecommunications providers, and provides the technologies to carriers.[316] Since June 2020, RoboKiller has introduced improvements to the service, including high volume "live-audio fingerprinting," to better combat neighbor spoofing and other tactics intended to obscure the true originating phone number; call screening, which is an optional feature that asks unknown callers their name and reason for calling before displaying the responses on the incoming call screen of the RoboKiller user; and configurable tiers of blocking protection that offer users greater control and flexibility.[317] Teltech is continuously optimizing its proprietary blocking algorithm based on the latest spam trends and will continue to release improvements and new features, including collecting and integrating STIR/SHAKEN signals into the blocking decisions, where applicable.[318] Teltech also released the Call Confidence API recently, allowing businesses and telecommunications providers to retrieve a real-time reputation score based on RoboKiller's proprietary data for a given phone number.[319]

88. The RoboKiller application immediately notifies users of all incoming calls that have been analyzed by RoboKiller, whether those are blocked, screened, or allowed.[320] For blocked calls specifically, the RoboKiller application provides users with details about each call, including the calling number, why it was blocked, and available label information to identify the call or calling party.[321] If a call is blocked mistakenly, users can add that number to their personal allow list and future calls from that number will be permitted to ring through.[322] This will also inform and update the RoboKiller algorithm.[323]

(Continued from previous page)

[309] *Id*. The Nomorobo mobile product sends the call directly to voicemail. *Id.* at 2.

[310] *Id.* at 1.

[311] CAPTCHA is an acronym for Completely Automated Public Turing Test to Tell Computers and Humans Apart and is a program that generates and grades tests that humans can pass but computer programs cannot.

[312] Nomorobo Letter at 2.

[313] Letter from Patrick Falzon, General Manager, Teltech Systems, Inc, to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 1 (May 21, 2021) (RoboKiller Letter).

[314] RoboKiller Letter at 1.

[315] *Id*.

[316] *Id*.

[317] *Id.* at 1-2.

[318] *Id.* at 2.

[319] *Id*.

[320] *Id*.

[321] *Id*.

[322] *Id*.

[323] *Id*.

89. *TNS.* TNS states that it provides the Call Guardian service, a robocall detection solution implemented by wireless carriers, broadband cable providers, and VoIP providers.[324] Over 105 million subscribers in the United States have Call Guardian.[325] Call Guardian uses information from over 1 billion signaling transactions per day on the TNS signaling network and IP call routing databases to differentiate legitimate calls from illegal and unwanted calls.[326] Call Guardian integrates this data with numerous other industry data sources, STIR/SHAKEN parameters, and crowd-sourced data, to analyze calls in real-time and determine a reputation score and category used by voice service providers.[327] Call Guardian constantly re-assesses calls, and notes suspicious behavior to keep pace with evolving tactics used by robocallers seeking to perpetrate scams.[328]

90. Call Guardian features Universal Call Blocking, which blocks tens of millions of illegal robocalls a month in the network before they ring on the customers' phones; Advanced Call Treatment sends likely illegal and unwanted calls to voicemail; and Advice of Risk warns subscribers about unwanted calls by displaying a spam indicator, which can be customized by each carrier, in their caller ID for suspicious calls.[329] Carriers choose where to "set the dial" for call blocking (e.g., based on high risk classification, nuisance classification, or particular scores assigned) and options for call handling (network level block, send to voicemail, complete, and label) to best serve their customers.[330] The Call Guardian services can be either opt-in or opt-out, and can be offered at various price points, including free to the consumer.[331]

91. According to TNS, fewer than 40% of wireless subscribers want all robocalls automatically blocked; almost 80% of consumers want their carrier to automatically block high-risk calls (those likely to be scams or fraud) while letting others pass through so they can choose whether to answer, send to voicemail, or block.[332] TNS asserts that almost 70% of consumers want lower-risk calls sent to voicemail, letting them control which messages to return.[333]

92. TNS estimates that, over the last 12 months, it and other analytics providers detected and alerted customers to over 77 billion likely illegal and unwanted robocalls.[334] At the same time, the overall volume of unwanted calls declined by 28% in 2020.[335] This decline likely is attributable to the Commission's enforcement actions, the expansion of call blocking by voice service providers, and disruptions in call centers caused by the COVID-19 pandemic.[336] According to TNS, almost 95% of high-risk calls originate from smaller voice service providers, up 3% from last year.[337] There has been

[324] TNS Comments at 3.

[325] *Id.*

[326] *Id.*

[327] *Id.*

[328] *Id.*

[329] *Id.* at 4.

[330] *Id.*

[331] *Id.*

[332] *Id.* at 5.

[333] *Id.*

[334] *Id.* at 6.

[335] *Id.*

[336] *Id.* at 6-7.

[337] *Id.* at 7.

significant progress in reducing illegal robocalls to wireless numbers; such calls to wireline numbers continue to be a problem—more than a third of the total calls (37%) to wireline telephone numbers are unwanted compared to 17% for wireless telephone numbers.[338] Spoofing of legitimate toll-free numbers continues to increase at a growing rate. Toll-free originated calls now account for 35% of the high-risk call volume, up from 28% in the second half of 2019; neighbor spoofing (i.e., spoofing a number to make it appear that the caller is local) declined by 43% from 2019 to 2020, while use of the same metropolitan area code to call a subscriber (near-neighbor spoofing) increased 17% in the same period.[339]

93. TNS confirms that, for IP calls, it provides SIP notification to the upstream carrier of call blocking.[340] TNS uses SIP code 603 or 607 to provide notifications. TNS does not yet provide notification for TDM calls.[341]

94. *YouMail.* YouMail explains that it offers a free call blocking app for mobile phones.[342] YouMail states that, since the First Call Blocking Report, it has continued to improve call-blocking tools and the back-end technology that detects unwanted callers at large in the public telephone network.[343] In addition to YouMail's client apps and direct-to-consumer offering, YouMail has recently included advanced tools for service providers to provide blocking features at the network level.[344] Every YouMail consumer can access call blocking features, which includes ringer protection, voicemail inbox protection, and call back protection.[345] YouMail's service directly protects over a million United States consumers per year, who have downloaded the free YouMail app, from unwanted, unsafe calls.[346] In addition, YouMail protects all Americans when the blocking is performed at the network level by service providers that have purchased access to YouMail's wholesale services.[347]

95. YouMail is considering offering advanced blocking features that would be offered for a fee, but has stated that it will continue to offer a free version of its product.[348] YouMail isates that it istplanning on improving direct consumer protection, as well as providing solutions for robocall mitigation by service providers; for example, one feature will reveal to consumers more information about the party behind these calls, such as mapping car warranty calls to a particular caller sending those calls and displaying that information to the consumer.[349]

---

[338] *Id*.

[339] *Id*.

[340] *Id.* at 8. A provider can attest to all IP-based calls that originate on or transit its network by adding a SIP header containing specific information, which is then transmitted in encrypted form with the call to the terminating provider. *Second STIR/SHAKEN Order*, 36 FCC Rcd at 1863-64, paras. 8-10.

[341] TNS Comments at 8.

[342] The app is available on YouMail's website or through the Apple App Store or Google Play. *See* YouMail, *Call Blocker, Block Spammers, Telemarketers and Unwanted Calls Forever*, https://www.youmail.com/home/feature/call-blocker (last visited June 15, 2021).

[343] Letter from Mike Rudolph, CTO, YouMail, Inc., to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 1 (Apr. 26, 2021) (YouMail Letter).

[344] YouMail Letter at 1.

[345] *Id*.

[346] *Id.* at 2.

[347] *Id*.

[348] *Id*.

[349] *Id.*

96. YouMail silences the ringing for calls that the consumer does not want; calls that analytics indicate are fraudulent or illegal go to voicemail.[350] For network-level solutions, YouMail offers controls where only calls carrying illegal content can be blocked from completion to a service provider's customers.[351] Consumers can choose from a variety of settings so that unwanted calls will not ring or can go to voicemail.[352] YouMail analyzes voicemail from unwanted calls to compare the content of the audio of those calls to "fingerprints" of known illegal and nuisance calls and determine if the ringer protection was appropriate.[353] In the case of a major bank's 800 number being spoofed, YouMail can take the audio content of those calls and match them to "fingerprints" known to belong to the actual bank to determine if the call is from an impersonator of that bank.[354]

97. Generally, YouMail is focused on illegal calls.[355] YouMail makes an effort to show the consumer every call; if there is a voicemail message, the audio is available along with the information about the nature of that call.[356] YouMail sends a message to the consumer's Android or iOS device to explain the block, such as a message indicating they were protected from a Social Security Administration imposter or a car warranty spammer.[357] If the caller left audio as part of the call, it is available for the consumer to access in their quarantined "Spam" folder to verify for themselves what was blocked.[358] Additionally, YouMail displays an ongoing counter of the quantity of recent protections (e.g., "you have been protected from [six] recent unwanted calls") and the consumer can drill into that message to see all the details for those calls.[359]

98. If the ringing on the device is incorrectly suppressed, YouMail has the voicemail message for that user; if it does not match known bad/illegal behavior, YouMail can send the call to the consumer's primary voicemail inbox to return the call.[360] At this time, the user will receive a push alert with a transcript of the call's content as well, so if the call was in fact an emergency alert or appointment reminder, it will display to the consumer.[361] Consumers can choose to receive an email whenever YouMail blocks a call or an email for every single voicemail or hang-up received on their behalf.[362]

99. YouMail observes that most consumer issues around unwanted callers involve callers who make their calls at low volume using a wide range of disposable numbers.[363] Because it is impractical to protect consumers at the device level for these types of calls, consumers are given a choice

[350] *Id.*

[351] *Id.*

[352] *Id.*

[353] *Id.* at 3.

[354] *Id.* at 4.

[355] *Id.* at 3.

[356] *Id.*

[357] *Id.*

[358] *Id.*

[359] *Id.*

[360] *Id.*

[361] *Id.*

[362] *Id.*

[363] *Id.* at 4.

to let unknown calls ring through to their voicemail where the "audio fingerprinting" algorithms can provide the protection against unwanted calls.[364]

C. Device Manufacturers' Blocking Services

100. *Apple*. Device manufacturer Apple's iPhones have an opt-in "Silence Unknown Callers" feature that, for iOS 13 and later, blocks phone numbers that are not saved in the user's contacts and that the user has not previously contacted.[365] Calls from unknown numbers are silenced and sent to voicemail, and appear in the recent calls list.[366]

101. *Google*. Google explains that it offers several tools for consumers, which do not require use of third-party applications.[367] Google provides each of the call authentication and blocking tools on an opt-in basis, and Google has no plans to offer network-level call blocking tools at this time.[368] One tool Google offers is the Phone app for Android, which provides visual warnings about potential spam callers, enables users to block specific numbers on their own devices, and allows users to report suspicious calls to help protect the Android community from fraud and spam.[369] The Google Phone app is free and can be preloaded by carriers on Android devices.[370] Google's Phone app can block suspected spam calls from ringing and instead send those calls directly to voicemail.[371] This feature is provided on an opt-in basis to users and builds on the "suspected spam caller" warning feature.[372] Users of the Phone app can see which calls were blocked by checking their log of received calls.[373] Google also provides the call-blocking tool on Google Voice, with similar features to those included in the Phone app, on an opt-in basis.[374] Most of Google's Pixel phones also offer a Call Screen feature, which gives users the option to have the Phone app ask who is calling and why, and to see a real-time transcript of the caller's response before deciding whether to answer a call.[375] This opt-in tool is free to Pixel users.[376]

IV. EFFECTIVENESS OF CALL BLOCKING TOOLS

A. False-Positive Blocks

102. We first examine the extent to which call blocking results in false positives. False positives are calls incorrectly identified as being spam or fraudulent and blocked in error. If a legitimate call is blocked, the consumer may miss a wanted call.

---

[364] *Id.*

[365] Apple, *Detect and Block Spam Phone Calls*, https://support.apple.com/en-us/HT207099 (last visited June 15, 2021).

[366] *Id.*

[367] Letter from Darah Franklin, Senior Counsel, Google LLC to G. Patrick Webre, Bureau Chief, Consumer and Governmental Affairs Bureau, FCC at 1 (Apr. 30, 2021) (Google Letter).

[368] Google Letter at 2.

[369] *Id.* at 1.

[370] *Id.*

[371] *Id.*

[372] *Id.*

[373] *Id.*

[374] *Id.*

[375] *Id.* at 2.

[376] *Id.*

103. *AT&T*. AT&T elicits feedback on AT&T Call Protect through a web portal.[377] Call originators who make calls that are blocked or labeled can use this web portal to submit a request for redress at no charge.[378] Based on user reports, fewer than one hundredth of one percent of calls are false positives.[379] When a blocked line calls an AT&T Mobility, FirstNet, U-verse, Prepaid, or Cricket customer, the caller receives the following announcement: "Your access to this network is restricted. Please contact 1-888-212-6040 if you feel you have reached this recording in error."[380] AT&T's Global Fraud Management Organization actively collects and investigates calls to this toll free number because calls could indicate a false positive, based on the complaints submitted to the toll free number.[381] However, AT&T estimates that the false-positive rate for its global fraud program is significantly less than 1%.[382] Out of approximately 113 telephone numbers that were the subject of complaints since April 2019, 110 of the complaints were deemed unsubstantiated upon investigation and, as a result, the telephone numbers remained blocked.[383] If a legitimate caller is blocked, the fraud team remediates and removes the block within 24 hours.[384]

104. *Bandwidth*. Bandwidth continues to experience false-positive blocking, and notes that overly-broad blocking practices risk interfering with communications services, which consumers demand must not be disregarded.[385] Bandwidth states that ensuring that illegal robocall prevention coexists with effective traffic delivery of legal calls across the communications ecosystem will depend upon the ongoing development of additional supplemental standards to the basic STIR/SHAKEN specifications now being implemented, together with other technical and operational best practices.[386] Bandwidth is concerned that, without a simultaneous adoption of standards that recognize and support myriad valid reseller models, end-users that rely upon IP-enabled services that incorporate underlying PSTN functions risk having their traffic improperly blocked or discriminated against.[387]

105. *First Orion*. First Orion estimates that its false-positive rate is a fraction of 1%.[388] First Orion proactively engages legitimate call originators in ways to help mitigate instances where calls are erroneously blocked or labeled.[389] First Orion has a website, https://www.calltransparency.com/, which allows call originators to register their outbound dialing numbers with First Orion.[390] First Orion, TNS, and Hiya have deployed www.freecallerregistry.com, a site that streamlines the registration process for call originators.[391] Registering either directly with an analytics engine or via the website also establishes

[377] AT&T Letter at 2-3. *See* Hiya, *Submit a Request*, https://hiyahelp.zendesk.com/hc/en-us/requests/new?ticket_form_id=824667 (last visited June 15, 2021). Calling parties can also reach Hiya's portal through http://www.att.com/reviewmycalllabel (last visited June 15, 2021).

[378] AT&T Letter at 3.

[379] *Id.*

[380] *Id.* at 4.

[381] *Id.*

[382] *Id.*

[383] *Id.*

[384] *Id.*

[385] Bandwidth Letter at 3.

[386] *Id.*

[387] *Id.*

[388] First Orion Letter at 3.

[389] *Id.* at 4.

[390] *Id.*

direct communication between call originators and the analytics engines for redress purposes.[392] First Orion states that, upon receipt of a redress request from a call originator, the vast majority of issues are resolved via research and investigation processes within hours—easily within the "reasonable" standard established by the Commission.[393]

106. *Hiya*. Hiya's service for AT&T Call Protect has a false-positive error rate at a fraction of a percent, based on reports by users.[394] Hiya also provides call originators a method to report and request redress of improperly flagged calls via the Hiya website.[395]

107. *Innovative Systems*. Innovative Systems explains that, with respect to false positives, out of the three million plus calls screened, only 3% were from numbers deemed "Friendly Callers."[396] For that small percentage of callers who could potentially fall into the false positive category, the service makes them easy to manage and add to an Allowed List on a case-by-case basis.[397]

108. *Nomorobo*. Nomorobo states that it has less than a .1% false positive rate.[398] Nomorobo allows parties to list numbers that were incorrectly blocked.[399]

109. *RoboKiller*. Teltech states that its main measure of effectiveness is based on an "agreement score," which accounts for the percentage of calls that were blocked, but which the consumer told them to allow in the future and calls that were allowed, but which the consumer told them to block in the future.[400] The agreement score is consistently over 99%, meaning fewer than 1% of calls received by RoboKiller users are reported as a false positive or false negative; all user feedback is automatically

(Continued from previous page)

[391] *Id.*; Hiya Letter at 4.

[392] First Orion Letter at 4.

[393] *Id.* To implement the requirement in section 10(b) of the TRACED Act to establish "effective redress options" for callers and consumers, the Commission's rules require terminating voice service providers that block calls to designate a single point of contact and resolve disputes in a reasonable amount of time consistent with industry best practice. *See* 47 CFR § 64.1200(k)(8); *Call Blocking Third Report and Order*, 35 FCC Rcd at 7633, 7634-35, paras. 51, 54-57. Subsequently, in the *Call Blocking Fourth Report and Order*, the Commission adopted requirements that terminating voice service providers (1) immediately notify the calling party when a call is blocked by sending either a SIP or ISDN User Part (ISUP) response code, as appropriate (and a corresponding requirement for all voice service providers in the call path to transmit these codes to the origination point), (2) disclose to subscribers a list of blocked calls upon request, (3) provide a status update regarding a blocked call within 24 hours if the block is disputed by the calling party, and (4) ensure that the point of contact established to handle blocking disputes also handles contacts from callers that are adversely affected by information provided by caller ID authentication and seeking to verify the authenticity of their calls. *Call Blocking Fourth Report and Order*, 35 FCC Rcd at 15238-47, para. 49-78. The first two requirements listed above have not taken effect as of the date of this report. The Commission declined to adopt a strict timeline for resolving disputed blocks. *Id*. at 15245-46, paras. 71-73.

[394] Hiya Letter at 3.

[395] *Id.* at 4. *See* Hiya, *Submit a Request*, https://hiyahelp.zendesk.com/hc/en-us/requests/new?ticket_form_id=824667 (last visited June 15, 2021).

[396] Innovative Systems Comments at 4.

[397] *Id.*

[398] Nomorobo Letter at 1.

[399] Nomorobo, *How Can I Allow a Call Nomorobo is Blocking to Ring Through?*, https://nomorobo.zendesk.com/hc/en-us/articles/205063319-How-can-I-allow-a-call-Nomorobo-is-blocking-to-ring-through- (last visited June 15, 20201); Nomorobo, *Send Us a Message*, https://www.nomorobo.com/contact (last visited June 15, 2021).

[400] RoboKiller Letter at 2.

captured by the blocking algorithm and used to inform future blocking decisions and self-correct as needed.[401]

110. *T-Mobile*. T-Mobile explains that the Scam Shield application allows customers to see when calls are blocked so they can report those calls by flagging the calls in the Scam Shield application, filling out a web form available at https://www.t-mobile.com/callreporting to report incorrectly blocked calls, or calling customer care.[402] T-Mobile investigates all customer reports of incorrectly blocked calls and, if the report is substantiated, T-Mobile removes the "scam" label and immediately stops blocking calls from that number.[403] T-Mobile encourages callers to register telephone numbers they believe to have been incorrectly blocked at www.calltransparency.com and to enter valid numbers assigned to them at www.freecallerregistry.com.[404]

111. *TNS*. According to TNS, very few end-users report that TNS incorrectly marked a call as a negative call.[405] Less than 0.2% of high-risk originating numbers are reported as having falsely been labeled as negative calls.[406] TNS also works with voice service providers and the analytics industry to provide easy and effective redress processes.[407] In addition to TNS' reportarobocall.com website[408] and carrier-branded websites used by TNS' customers, TNS and other analytics companies created www.freecallregistry.com as a single source for callers to register their numbers with all three major analytics providers at once.[409] On all sites, TNS provides a response to call blocking redress requests within 24 hours and provides feedback on most call labeling requests within two business days.[410]

112. *UScellular*. UScellular states that, if a blocked caller believes calls are being blocked in error, the caller can address its concern to the contact provided on the UScellular website; this directs a query to TNS, who investigates and responds to the query as appropriate.[411] According to TNS, approximately 0.25% of originating numbers are reported as having falsely been labeled as negative calls.[412]

113. *Verizon*. Verizon states that the rate of false positives, meaning calls incorrectly identified as spam or fraud, for Call Filter is fewer than 0.2% of originating numbers identified as high-risk robocalls are reported as having been incorrectly blocked.[413] Verizon currently sends Release Code 603 ("denied") for calls blocked by the network blocking programs so that the originating carrier and/or the caller are aware of the blocks.[414] Verizon also provide calling parties with the opportunity to contest

[401] *Id.*

[402] T-Mobile Letter at 3.

[403] *Id.*

[404] *Id.* at 4.

[405] TNS Comments at 8.

[406] *Id.*

[407] *Id.* at 9.

[408] TNS, Call Guardian, *Welcome to TNS' Robocall Feedback Website!*, https://reportarobocall.com/trf/ (last visited June 15, 2021).

[409] TNS Comments at 9.

[410] *Id.*

[411] UScellular Letter at 2.

[412] *Id.*

[413] Verizon Letter at 4.

[414] *Id.* at 6.

any purportedly incorrect blocks via its feedback website, https://www.voicespamfeedback.com/vsf/.[415] Additionally, Verizon sends daily automated emails to upstream wholesale customers to inform them of the top 10 invalid numbers that were blocked to educate them about the need to promote hygienic calling behavior.[416]

114. *YouMail*. Consumers can tell YouMail if a call was incorrectly sent into spam.[417] YouMail explains that false positives are generally automatically rectified if the caller presents audio information that no longer matches "audio fingerprints" that are known to be illegal, fraudulent, or nuisance, or if the consumer reports a call as "not spam."[418]

B. Issues from Callers Regarding False-Positive Blocks

115. The American Bankers Association (ABA) contends that its members report that they continue to experience incorrect labeling of their numbers and erroneous blocks of their outbound calls.[419] According to ABA, one large bank reported that, in March 2021, two phone numbers that the bank used to place outbound calls (and that were registered with the major voice service providers) were mislabeled as spam by three major providers.[420] The numbers remained mislabeled for 14 days after the bank made its request for redress; approximately 779,684 outbound calls were mislabeled as spam and/or calls from those numbers blocked.[421] ABA observes that a second large bank reported that, between October 2020 and March 2021, it experienced 38 occasions during which outbound numbers used by the bank were labeled as spam by three major voice service providers; it had to contact the originating provider and, on occasion, other providers in the call's pathway to resolve the mislabeling.[422] According to ABA, a third large bank reported that, in May 2020, a voice service provider's third-party call-labeling service provider mislabeled a phone number used by the bank's automobile lending division as spam, resulting in the blocking of collections-related calls from that number.[423]

116. The Heartland Credit Union Association (HCUA) and the Credit Union National Association (CUNA) observe that credit unions have experienced increased rates of call blocking or mislabeling, and determining that calls are blocked is difficult in the absence of notification.[424] HCUA contends that some larger credit unions were able to identify that their calls were being blocked by the service providers and some credit unions have discovered through conversations with their members that their calls are being labeled as potential spam or suspected spam.[425] CUNA states that credit unions were able to discover that calls were being blocked through the use of calling technologies that report an increase in busy signals and, upon investigation, these calls were identified as having been blocked by service providers.[426] One large credit union identified over 100,000 blocked calls.[427]

---

[415] *Id.*

[416] *Id.*

[417] YouMail Letter at 3.

[418] *Id.* at 4.

[419] ABA Comments at 2.

[420] *Id.*

[421] *Id.*

[422] *Id.* at 3.

[423] *Id.*

[424] CUNA Comments at 1; HCUA Comments at 1.

[425] CUNA Comments at 2; HCUA Comments at 1.

[426] CUNA Comments at 2.

117. According to HCUA, the experience of these credit unions is consistent with that of numerous other industries that have reported that legitimate and often critical calls were being blocked or mislabeled as spam or scam calls,[428] such as calls alerting individuals of a potential wildfire;[429] calls from banks, including attempts to alert customers of potential fraud or to conduct "wellness checks" during the COVID pandemic;[430] calls from correctional facilities by incarcerated persons to their families;[431] and calls from alarm companies to customers or public safety agencies in response to an alarm signal.[432] Credit unions also consistently report that, when they speak with service providers about erroneous call blocking and call labeling, service providers indicate that analytics tools identify these credit union calls as potential spam based solely on the quantity of outbound calls being placed by the credit union.[433]

118. TCN, Inc. (TCN) states that, in May 2020, it noted that voice service providers were regularly over-blocking a wide array of calls.[434] According to TCN, over the past year, voice service providers continue to block lawful calls; for example, a large hospital that relies on voice service to communicate appointment reminders and other healthcare-related information to patients routinely experienced erroneous call-blocking every few weeks and the relevant voice service providers have not implemented a redress procedure pursuant to the TRACED Act's or Commission's requirements.[435] TCN states that the Commission must ensure that carriers adhere to the Commission's established deadline of January 1, 2022, for sending the appropriate SIP or ISUP codes to parties whose calls are blocked.[436] Receipt of a SIP or ISUP code will provide an important tool for parties to: (1) appropriately engage a voice service provider's redress mechanism; (2) resolve blocking misunderstandings or mistakes; and (3)

(Continued from previous page)
[427] *Id.*

[428] CUNA Comments at 2; HCUA Comments at 1.

[429] CUNA Comments at 3; HCUA Comments at 1.

[430] CUNA Comments at 2.

[431] *Id.*

[432] *Id.* at 3.

[433] *Id.* at 2.

[434] TCN Comments at 3.

[435] *Id.* at 3. In the *Call Blocking Fourth Report and Order*, adopted on December 29, 2020 and released on December 30, 2020, the Commission adopted requirements that terminating voice service providers immediately notify the calling party when a call is blocked by sending either a SIP or ISDN User Part response code and that all voice service providers in the call path transmit these codes to the origination point so that the callers receive timely notice of the block; that terminating voice service providers disclose to subscribers a list of blocked calls upon request; and that terminating voice service providers provide a status update regarding a blocked call within 24 hours if the block is disputed by the calling party. *Call Blocking Fourth Report and Order*, 35 FCC Rcd at 15238-245, paras. 48-69. The Commission declined to adopt a strict timeline for resolving disputed blocks. *Id*. at 15245-46, paras. 71-73. The Commission also declined to adopt redress requirements for labeling disputes. *Id*. at 15248, paras. 79-81. The effective date for the rule requiring immediate notification of blocked calls is January 1, 2022. *Id*. at 15242, para. 61. The effective date for the remaining requirements is May 6, 2021, except the requirement to report to the Commission following notification of unlawful traffic and to disclose the list of blocked calls which require OMB approval (§ 64.1200(k)(10) and (n)(2)); the Commission will publish a document in the Federal Register announcing the effective date for those sections.

[436] TCN Comments at 5. In the *Call Blocking Fourth Report and Order*, adopted on December 29, 2020, and released on December 30, 2020, the Commission adopted requirements that terminating voice service providers immediately notify the calling party when a call is blocked by sending either a SIP or ISDN User Part response code and that all voice service providers in the call path transmit these codes to the origination point so that the callers receive timely notice of the block. *Call Blocking Fourth Report and Order*, 35 FCC Rcd at 15239-242, paras. 52-61. The effective date for this rule is January 1, 2022. *Id*. at 15242, para. 61.

reach consumers with the time-sensitive information that prompted the call.[437] TCN contends that, of the 10 voice service providers that it polled in April 2021, none affirmatively responded that they established redress procedures for calling parties.[438]

V. STATE OF DEPLOYMENT OF CALLER ID AUTHENTICATION

119. Pursuant to the *2019 Call Blocking Declaratory Ruling*, this second report includes information on the state of deployment of caller ID authentication through implementation of the STIR/SHAKEN framework, and contain "snapshots" of deployment and implementation of Commission and industry efforts at the time of its release.[439] The first report summarized the state of implementation up to June 2020 following the release of the March 2020 *STIR/SHAKEN Order*, in which the Commission first mandated implementation of the STIR/SHAKEN call authentication framework.[440] In this report, we provide updates on progress made by industry toward implementing STIR/SHAKEN in light of the June 30, 2021 implementation deadline.

A. STIR/SHAKEN Implementation Background

120. *Technical Background.* To combat illegal spoofing, industry technologists developed the STIR/SHAKEN caller ID authentication framework to allow for the authentication and verification of caller ID information for calls carried over IP networks.[441] The STIR/SHAKEN framework relies on public key cryptography to securely transmit the information that the originating voice service provider knows about the identity of the caller and its relationship to the phone number it is using throughout the entire length of the call path, allowing the terminating voice service provider to verify the information on the other end.[442] The framework relies on digital "certificates" to ensure trust; these communicate, in essence, that the voice service provider is the entity it claims to be and that it has the right to authenticate the caller ID information.[443] A governance framework establishes a structure for certificate assignment and management, including the role of the Governance Authority, which defines the policies and procedures for which entities can issue or acquire certificates,[444] and the Policy Administrator, which applies those rules and confirms that voice service providers are authorized to request and receive certificates.[445] After registering with and receiving authorization from the Policy Administrator, a voice

[437] TCN Comments at 5.

[438] *Id.* at 6. We note that the effective date for the notification of a block and response code is January 1, 2022. *Call Blocking Fourth Report and Order*, 35 FCC Rcd at 15242, para. 61.

[439] *2019 Call Blocking Declaratory Ruling*, 34 FCC Rcd at 4904, paras. 87-89.

[440] *See First Call Blocking Report* at 30-34.

[441] *Second STIR/SHAKEN Order*, 36 FCC Rcd at 1862, para. 6. A working group of the Internet Engineering Task Force (IETF), called the Secure Telephony Identity Revisited (STIR), developed several protocols for authenticating caller ID information. *Id*. The Alliance for Telecommunications Industry Solutions (ATIS), in conjunction with the SIP Forum, produced the Signature-based Handling of Asserted information using toKENs (SHAKEN) specification, which standardizes how the protocols produced by STIR are implemented across the industry. *See id.* at 1862-63, para. 7.

[442] *Second STIR/SHAKEN Order*, 36 FCC Rcd at 1863, para. 8.

[443] *STIR/SHAKEN Order*, 35 FCC Rcd at 3246, para. 9.

[444] This role is currently filled by the Secure Telephone Identity Governance Authority (STI-GA). Secure Telephone Identity Governance Auth., *Secure Telephone Identity Governance Authority*, https://sti-ga.atis.org (last visited June 15, 2021).

[445] The Governance Authority selected iconectiv to fill this role. Press Release, ATIS, Mitigating Illegal Robocalling Advances with Secure Telephone Identity Governance Authority Board's Selection of iconectiv as Policy Administrator (May 30, 2019), https://www.atis.org/press-releases/mitigating-illegal-robocalling-advances-with-secure-telephone-identity-governance-authority-boards-selection-of-iconectiv-as-policy-administrator.

service provider may receive its certificate and begin participating in the exchange of traffic with caller ID information that has been authenticated consistent with STIR/SHAKEN. Thus, to participate in STIR/SHAKEN, a voice service provider must not only complete necessary upgrades to its network infrastructure to be able to authenticate and verify caller ID information, it must also complete registration through the governance system.[446]

121. *Regulatory Action.* In the March 2020 *STIR/SHAKEN Order*, the Commission, acting pursuant to the TRACED Act, mandated that voice service providers implement STIR/SHAKEN on their IP networks by June 30, 2021.[447] In the September 2020 *Second STIR/SHAKEN Order*, the Commission implemented an exemption from the STIR/SHAKEN mandate for providers that began implementation of caller ID authentication early, granted extensions of the mandate to certain categories of voice service providers, and established rules regarding robocall mitigation by providers subject to an extension.[448]

122. *Exemptions from the Implementation Mandate.* The TRACED Act directed the Commission to exempt from its caller ID authentication implementation mandates voice service providers that the Commission determined met certain early implementation benchmarks in their IP networks.[449] To receive the exemption, the Commission established that a voice service provider must meet the following requirements: (i) have undertaken the network preparations necessary to deploy the STIR/SHAKEN protocols on its network; (ii) have completed formal registration (including payment) and testing with the Policy Administrator; (iii) have completed the necessary network upgrades to at least one network element to enable the authentication and verification of caller ID information consistent with the STIR/SHAKEN standards; and (iv) reasonably foresee that it will have completed all necessary network upgrades to its network infrastructure to be able to authenticate and verify caller ID information for all IP calls exchanged with STIR/SHAKEN-enabled partners by June 30, 2021.[450] It required a voice service provider seeking an extension to file a certification explaining in detail how it met the criteria necessary for an exemption by December 1, 2020, and directed the Wireline Competition Bureau to review the certifications and issue a list of parties that filed complete certifications and received the exemption by December 30, 2020.[451]

123. *Extensions of the Implementation Deadline and Robocall Mitigation*. The TRACED Act created a process by which the Commission could grant extensions of the June 30, 2021, implementation deadline for voice service providers the Commission determined faced "undue hardship" in implementing STIR/SHAKEN.[452] After assessing the burdens and barriers faced by different classes of voice service providers, the Commission granted four class-based extensions.[453] The TRACED Act further directed the Commission to require all voice service providers with an extension to "implement an appropriate

---

[446] *See Second STIR/SHAKEN Order*, 36 FCC Rcd at 1914-15, para. 113; *see also STIR/SHAKEN Order*, 35 FCC Rcd at 3257, para. 32.

[447] *STIR/SHAKEN Order*, 35 FCC Rcd at 3243, para. 3.

[448] *See Second STIR/SHAKEN Order*, 36 FCC Rcd 1859.

[449] TRACED Act § 4(b)(2).

[450] 47 CFR § 63.6403(a); *Second STIR/SHAKEN Order*, 36 FCC Rcd at 1912-15, paras. 106-13.

[451] *Second STIR/SHAKEN Order*, 36 FCC Rcd at 1917, para. 119.

[452] TRACED Act § 4(b)(5)(A)(ii).

[453] Specifically, the Commission granted the following class-based extensions: (1) a two-year extension to small voice service providers; (2) an extension to voice service providers that cannot obtain a "certificate" until such providers are able to obtain one; (3) a one-year extension to services scheduled for section 214 discontinuance; and (4) a continuing extension for the parts of a voice service provider's network that rely on technology that cannot initiate, maintain, and terminate SIP calls until a solution for such calls is readily available. *See* STIR/SHAKEN *Order*, 36 FCC Rcd at 1877-83, 1892-96, paras. 40-51, 66-70; 47 CFR §§ 64.6304(a)-(d).

robocall mitigation program to prevent unlawful robocalls from originating on the network of the provider."[454] The Commission required voice service providers subject to an extension to certify the methods they are using to combat the origination of illegal robocalls and announced that it would establish a database for these certifications.[455] The Commission also required "all voice service providers—not only those granted an extension—to file certifications with the Commission regarding their efforts to stem the origination of illegal robocalls on their networks."[456] Specifically, the Commission required all voice service providers to certify that their traffic is either fully, partially, or not yet signed with STIR/SHAKEN.[457] On April 20, 2021, the Wireline Competition Bureau announced voice service providers could begin submitting certifications to the Robocall Mitigation Database.[458] The deadline for submitting certifications to the database is June 30, 2021.[459] Intermediate providers and terminating voice service providers will be prohibited from accepting traffic directly from voice service providers not listed in the Robocall Mitigation Database beginning September 28, 2021.[460]

124. *December 2020 Implementation Report.* On December 29, 2020, pursuant to the TRACED Act,[461] the Wireline Competition Bureau released a report to Congress on voice service providers' progress to implement caller ID authentication technology on their IP networks.[462] The report focused on three categories of voice service providers: (1) those that implemented STIR/SHAKEN and began exchanging signed traffic with other voice service providers; (2) voice service providers that implemented STIR/SHAKEN but had not yet begun exchanging signed traffic with other voice service providers; and (3) voice service providers that had achieved limited, if any, progress towards upgrading their networks to support STIR/SHAKEN.[463] In the first category, the Bureau reported that 72 voice service providers had registered with the Policy Administrator and were authorized to participate in STIR/SHAKEN through the governance system.[464] Among those 72 were seven voice service providers that filed for, and received, exemptions from the implementation mandate: AT&T Services Inc. (AT&T), Bandwidth Inc. (Bandwidth), Charter Communications, Inc. (Charter), Comcast Cable Communications, LLC (Comcast), Cox Communications, Inc. (Cox), Cellco Partnership, d/b/a Verizon Wireless (Verizon Wireless), and Vonage Holding Corp. (Vonage).[465] Lumen (formerly CenturyLink) and T-Mobile also announced they had implemented STIR/SHAKEN and begun exchanging authenticated traffic with other

[454] TRACED Act § 4(b)(5)(C).

[455] *Second STIR/SHAKEN Order*, 36 FCC Rcd at 1902-03, paras. 82-85.

[456] *Id.*, 36 FCC Rcd at 1902, para. 82.

[457] *Id.*, 36 FCC Rcd at 1902, para. 82; 47 CFR §§ 64.6305(b)(1)(i)-(iii).

[458] *See Wireline Competition Bureau Announces Opening of Robocall Mitigation Database and Provides Filing Instructions and Deadlines*, Public Notice, WC Docket No. 17-97, DA 21-454 (WCB Apr. 20, 2021) (*Robocall Mitigation Database Public Notice*).

[459] *Id.* at 1.

[460] *Id.*; *see Second STIR/SHAKEN Order*, 36 FCC Rcd at 1904, para. 86; 47 CFR § 64.6305(c).

[461] TRACED Act § 4(b)(3).

[462] FCC, Report to Congress on Caller ID Authentication Implementation Process (2020), https://docs.fcc.gov/public/attachments/DOC-368981A1.pdf (December Report).

[463] *Id.* at 7.

[464] *Id.*

[465] December Report at 7; *see Wireline Competition Bureau Announces Seven Voice Service Providers Qualified for STIR/SHAKEN Exemption*, Public Notice, WC Docket Nos. 17-97, 20-68, 35 FCC Rcd 14830 (WCB 2020) (*Exemptions Public Notice)*. Only AT&T's Wireline IP network received the exemption. *Id.* at 2 n.10.

Tier-1 voice service providers, though neither sought an exemption.[466] In the second category, the Bureau reported that numerous voice service providers, including Brightlink, Buckeye Broadband, Frontier, Google Verified Calls, Inteliquent, Peerless Network, Twilio, Quality Voice & Data, Viaero Wireless, and Ytel reported they had implemented STIR/SHAKEN but had not announced they had begun exchanging signed traffic.[467] Finally, the report identified a selection of providers that had released statements regarding STIR/SHAKEN but had not yet announced they had implemented the framework.[468]

B. Updates on STIR/SHAKEN Deployment and Implementation

125. Voice service providers have made progress towards STIR/SHAKEN implementation since the Wireline Competition Bureau released its December report. First, beginning April 20, 2021, voice service providers were able to submit certifications to the Robocall Mitigation Database and self-report the level of STIR/SHAKEN implementation they have achieved. To date, 1327 voice service providers have filed certifications. Two hundred and seven of these voice service providers have certified to complete STIR/SHAKEN implementation; 290 to partial STIR/SHAKEN implementation; and 830 to no STIR/SHAKEN implementation.[469] The deadline for filing these certifications is June 30, 2021, after which point the Commission will have comprehensive data on the state of implementation across the industry.

126. Second, as we have explained, voice service providers must register with and receive authorization from the Policy Administrator in order to exchange STIR/SHAKEN authenticated traffic. At the time of the release of this report 288 voice service providers were registered with the Policy Administrator.[470] Since the December Report was released, 261 providers have registered, suggesting accelerated industry adoption since December 2020 as the June 30 deadline approaches. This number also suggests early implementation by some small voice service providers despite the fact they received a two-year extension to implement STIR/SHAKEN.[471] As the Commission has previously explained,[472] from 2014 to 2018, providers that make the initial long-distance call path choice for more than 100,000 domestic retail subscriber lines were obligated to file rural call completion reports and 55 providers filed such reports in 2017.[473] That a total of 288 providers registered with the Policy Administrator implies that approximately 230 voice service providers with fewer than 100,000 lines have already obtained certificates from the STI-GA.

127. Third, third party data show industry has been steadily progressing toward increased implementation. For instance, TNS "found that more than one-third of the total calls it analyzed in

[466] December Report at 8-9.

[467] *Id.* at 9-10.

[468] *Id.* at 10-11; *see id.* at 11 n.83.

[469] FCC, *Robocall Mitigation Database,* https://fccprod.servicenowservices.com/rmd?id=rmd_listings (last visited June 22, 2021).

[470] iconectiv, *Authorized Service Providers*, https://authenticate.iconectiv.com/authorized-service-providers-authenticate (last visited June 22, 2021).

[471] *See Second STIR/SHAKEN Order*, 36 FCC Rcd at 1877, para. 40.

[472] *See STIR/SHAKEN Third FNPRM*, FCC 21-62, at para. 17.

[473] *See Rural Call Completion*, WC Docket No. 13-39, Report, 32 FCC Rcd 4980, 4985, para. 12 (2017) (noting that approximately 55 providers filed rural call completion reports over the prior two years); 47 CFR § 64.2101 (defining "covered providers" required to file reports as any provider that "makes the initial long-distance call path choice for more than 100,000 domestic retail subscriber lines, counting the total of all business and residential fixed subscriber lines and mobile phones and aggregated over all of the providers' affiliates"). The Commission eliminated this reporting requirement in 2018. *See Rural Call Completion*, WC Docket No. 13-39, Second Report and Order and Third Further Notice of Proposed Rulemaking, 33 FCC Rcd 4199, 4224-27, paras. 58-64 (2018).

December 2020 were self-signed, up from 21% in the beginning of the year."[474]

128. Fourth, large voice service providers have reported additional progress toward STIR/SHAKEN implementation. Several voice service providers that received exemptions due to early implementation progress have continued to report additional progress. Charter reports it "completed its implementation of the STIR/SHAKEN Authentication framework across its entire [IP] network in December 2019."[475] Comcast estimates it is now signing "virtually all calls originating from Comcast residential voice customers and small- and medium-sized business voice customers, and as of March 2021, approximately 30% of all calls originating from other providers and bound for such customers are signed and verified."[476] Similarly, in March 2021, T-Mobile announced it completed STIR/SHAKEN interconnection with "all other major networks"[477] and states it "now authenticates calls with wireless and network providers that collectively represent about 98% of wireless customers in the U.S."[478] Verizon also announced in March 2021 that it was "now exchanging STIR/SHAKEN-enabled calls with major wireless carriers that "collectively represent around 80% of the U.S. wireless industry" as well as a "major wireline provider."[479] Voice service providers that did not receive exemptions also report progress toward implementation, with NCTA-The Internet & Television Association reporting that its members that did not receive exemptions are "on track to meet the Commission's June 30, 2021 implementation deadline."[480] Frontier claims it "has deployed STIR/SHAKEN on its IP network and has already begun exchanging authenticated STIR/SHAKEN traffic with several carriers."[481] Similarly, Lumen states that "over the past several months, we have been hard at work implementing STIR/SHAKEN call authentication technology on the IP portions of our network in order to meet the June 30, 2021 implementation deadline mandated by the TRACED Act."[482] UScellular states it initially introduced SITR/SHAKEN in 2019 and is "now interconnecting with more carriers via SIP and exchanging STIR/SHAKEN information."[483] And Five9, a cloud contact provider, reported it partnered with Neustar to implement STIR/SHAKEN call authentication for its customers ahead of the June 30 deadline.[484]

129. Fifth, voice service providers have explained how they are using and intend to use STIR/SHAKEN information to protect their subscribers. AT&T reports that it "has integrated the STIR/SHAKEN verification results into its call blocking analysis" and "intends to share with consumers the STIR/SHAKEN verification results to the extent" feasible.[485] Charter explains that its "Call Guard"

---

[474] TNS Letter at 6; Transaction Network Services Inc., TNS 2021 Robocall Investigation Report at 21 (2021), https://tnsi.com/forms/tns-2021-robocall-report/ (TNS 2021 Robocall Report).

[475] Charter Letter at 2.

[476] Comcast Letter at 3.

[477] Press Release, T-Mobile, T-Mobile Completes STIR/SHAKEN with ALL Major Carriers to Help Protect Customers from Scams and Spam (Mar. 25, 2021), https://www.t-mobile.com/news/network/stir-shaken-all-networks.

[478] T-Mobile Letter at 5.

[479] Press Release, Verizon, Verizon Works with wireless carriers in US to combat robocalls (Mar. 17, 2021), https://www.verizon.com/about/news/verizon-carriers-combat-robocalls.

[480] NCTA Comments at 2.

[481] Frontier Letter at 1.

[482] Lumen Letter at 1.

[483] UScellular Letter at 5.

[484] Press Release, Five9, Five9 Partners with Neustar to Support STIR/SHAKEN Framework for Restoring Trust in Voice Communication (May 11, 2021), https://www.five9.com/news/news-releases/stirshaken.

[485] AT&T Letter at 4-5.

robocall blocking solution, which its offers "by default to Spectrum Voice and Spectrum Business Voice customers," uses "STIR/SHAKEN call-authentication information, and predictive call-pattern analytics to assess every incoming call and apply a score to each based on its measured level of risk."[486] Comcast states that, in March 2021, it launched its Verified Caller ID service that uses STIR/SHAKEN authentication information to display a verification message to customers "any time the caller's voice provider has confirmed that the call is coming from a legitimate telephone number."[487] UScellular states its VoLTE-enabled subscribers can utilize the TNS "Call Guardian" application that utilizes "STIR/SHAKEN verification status" and other information "to determine the likelihood that a call is unwanted or potentially fraudulent."[488] And Verizon explains that its "Verizon Call Filter" feature uses "a call's STIR/SHAKEN verification results as one component of the more holistic real-time analysis to determine whether to block or label a call."[489]

VI. IMPACT ON 911 AND PUBLIC SAFETY

130. Commenters generally recognize and underscore the important dual goals of protecting public safety entities from unwanted robocalls while ensuring that call blocking efforts do not interfere with emergency services, including both consumer calls to 911 and return calls from PSAPs to consumers.[490] Several commenters further detail the measures undertaken in support of these goals. For example, AT&T states that when it is made aware of a suspect calling event impacting a public safety line, it takes steps to mitigate, if not eliminate, the impact on the public safety entity.[491] Charter recites that it has a process through which PSAP personnel and law enforcement can, 24 hours a day, seven days a week, report any problems with emergency calls or make other requests.[492]

131. While no public safety entities submitted comments for this report, we have previously noted concerns with inadvertent blocking of emergency calls.[493] Commenters suggest that there have been few instances of this situation occurring.[494] Where it has occurred, and where most efforts have been directed, is with respect to call-backs from PSAPs to 911 callers. AT&T, for example, states that it is not aware of any incidents where calls to 911 were unintentionally blocked, but describes two situations in 2020 in which a call-back from a PSAP was initially blocked. In those cases, the PSAP inserted "911" in the caller ID, but because 911 is considered an invalid originating phone number the call was initially blocked. In both instances, AT&T states that outreach to the PSAP resolved the problem when the PSAP changed the outbound caller ID from 911 to a valid 10-digit telephone number.[495] Verizon states that it directs legitimate callers to their analytic engine's website so that they can efficiently register their

[486] Charter Letter at 1-2.

[487] Comcast Letter at 3-4.

[488] UScellular Letter at 2.

[489] Verizon Letter at 7.

[490] *See, e.g.*, AT&T Letter at 5; Charter Letter at 2; Comcast Letter at 4; Cox Comments at 4; NCTA Comments at 3.

[491] AT&T Letter at 5.

[492] Charter Letter at 2.

[493] First Call Blocking Report at para. 78.

[494] First Orion, for example, states that it is not aware of any instances of unintentional blocking of calls to 911. First Orion Letter at 5; *see also,* TNS Comments at 11; RoboKiller Letter at 3; YouMail Letter at 5. Nomorobo similarly states that it is not aware of any blocking incidents for calls to or from 911. Nomorobo Letter at 2; *see also,* UScellular Letter at 4 (no UScellular network-originated 911 calls have been blocked and UScellular is not aware of any unintentionally blocked 911 call backs); Cox Comments at 4; T-Mobile Letter at 5; Verizon Letter at 7-8.

[495] AT&T Letter at 5.

numbers to ensure they will be treated appropriately, and takes action to ensure that legitimate public safety-related calls would trigger correct caller ID information.[496] While Verizon also states it is not aware of instances where emergency calls to or from PSAPs have been inadvertently blocked, they indicate that in a few cases Verizon has been alerted to a "labeling issue" affecting an outbound dialing number from a local PSAP.[497] Verizon indicates that it is working with a vendor to identify administrative numbers for PSAPs across the United States.[498]

132. Comcast states it is engaging with public safety and emergency services to minimize the risk of accidental blocking.[499] Charter also indicates that it works with PSAPs, including educating them about new or emerging call-blocking tools to help ensure that it does not inadvertently block their calls. Charter also provides a dedicated email address for PSAPs to proactively notify Charter of administrative lines that may generate high volumes of calls, or originate from incomplete or invalid telephone numbers, so it can document those numbers and avoid inadvertently blocking or mislabeling them as spam.[500] T-Mobile states that after a customer calls 911, T-Mobile deactivates Scam ID and Scam Block on all inbound calls for a period to avoid inadvertently blocking a PSAP returning a 911 call.[501] Verizon similarly states that when a Verizon subscriber calls 911, blocking of inbound calls is disabled for a period of time to ensure that customers do not miss call-backs from the emergency services provider.[502] Innovative Systems states that all numbers that correspond with emergency services entities, including 911, are pre-configured to the allowed list and will never be blocked by the screening service.[503]

133. In this regard, RoboKiller similarly opines that it is possible that call-blocking technology could unintentionally block a call-back from a 911 operator.[504] It states that there is no comprehensive list of PSAP administrative numbers available today, and therefore call blocking services have no mechanism for automatically ensuring the delivery of calls from these numbers.[505] While RoboKiller asserts that use of "live audio-fingerprinting" significantly reduces this risk, as it does not rely solely on caller ID based methods, Robokiller believes that the development of a centralized list of PSAP administrative numbers would benefit consumers.[506]

134. TNS states that it has built a database to assist in identifying outbound numbers used by public safety entities.[507] In this respect, TNS indicates that it has worked with the National Emergency Number Association (NENA), to explore ways that TNS can obtain information from PSAPs regarding

[496] Verizon Letter at 4.

[497] Verizon Letter at 8.

[498] *Id.*

[499] Comcast Letter at 4.

[500] Charter Letter at 3. Charter also states that it participates in ATIS and other technical groups, which are considering standards for authenticating public safety calls to more broadly help prevent inadvertent blocking of public safety numbers.

[501] T-Mobile Letter at 5.

[502] Verizon Letter at 8. *See also,* YouMail Letter at 4-5 (YouMail recognizes that it could enhance its service whereby following an outbound call to 911, it could completely disable incoming call blocking for a period of time after that call is made).

[503] Innovative Systems Comments at 5.

[504] RoboKiller Letter at 3.

[505] *Id.*

[506] *Id.*

[507] TNS Comments at 11.

the numbers that they use to facilitate outreach to the 911 community.[508] In some cases, TNS indicates that its carrier partners conducted outreach to PSAPs in their service territories, asking for assistance in identifying numbers that they use to originate outbound calls, such as call-back services or "reverse 911" messages.[509]

VII. CONCLUSION

135. According to Hiya, 94% of all unknown calls went unanswered in 2020.[510] Experience has trained consumers to not answer unidentified calls because they are often spam or fraud, so legitimate callers are suffering.[511] The Commission has devoted significant resources to fighting illegal and unwanted robocalls and the industry has made tremendous strides in providing tools for consumers to block unwanted and illegal calls. This Second Call Blocking Report summarizes information from voice service providers and third-party analytics companies and concludes that they offer improved call blocking services to their customers through updated analyses of potentially illegal calls and more blocking tools. More illegal and unwanted calls are blocked by voice service providers at the network level and with opt-in and opt-out tools offered to customers. The Commission recognizes that despite these advances, more work needs to be done and remains committed to working with the industry and other government agencies to eliminate unwanted and illegal robocalls.

[508] *Id.* TNS further states that it compiled thousands of numbers associated with public health entities in order to facilitate the proper transmission of COVID-19-related emergency calls to assist in identifying public safety calls outside of the COVID-19 pandemic.

[509] TNS Comments at 12.

[510] Hiya Letter at 4.

[511] *Id.*

APPENDIX

Parties that submitted comments in response to the Public Notice and those who responded to letters

Commenter	Abbreviated Name
American Bankers Association	ABA
AT&T Services, Inc.	AT&T
Bandwidth Inc.	Bandwidth
William M. Bird	Bird
Charter Communications	Charter
Comcast Corporation	Comcast
Cox Communications, Inc.	Cox
Credit Union National Association	CUNA
First Orion Corp.	First Orion
Frontier Communications	Frontier
Google LLC	Google
Heartland Credit Union Association	HCUA
Hiya, Inc.	Hiya
INCOMPAS	INCOMPAS
Innovative Systems LLC	Innovative Systems
Lumen Technologies	Lumen
NCTA--The Internet and Television Association	NCTA
TCN, Inc	TCN
TDS Telecommunications LLC	TDS Telecom
Telephone Science Corp. d/b/a Nomorobo	Nomorobo
Teltech Systems, Inc.	Teltech or RoboKiller
T-Mobile USA,Inc.	T-Mobile
Transaction Network Services, Inc.	TNS
United States Cellular Corporation	UScellular
USTelecom—The Broadband Association	USTelecom
Verizon Communications Inc.	Verizon
Vonage Holdings Corp.	Vonage
YouMail, Inc.	YouMail